ICANN83 | PF – GNSO: CPH DNS Abuse Community Update
Monday, June 09, 2025 – 13:45 to 15:00 CEST

SUE SCHULER: Hello, and welcome to the CPH DNC Abuse Community Update. My name is Sue, and I'm a participation manager for this session. Please note that the session is being recorded and is governed by the ICANN expected standards of behavior and the ICANN community anti-harassment policy. 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. Onside participants will use a physical microphone to speak. Please state your name for the record and speak at a reasonable space. I will now hand the floor over the Dennis Tan and Chris Disspain.

DENNIS TAN: Thank you, this is Dennis Tan for Verisign and I'm one of the colleagues of the CPH DNS Abuse Working Group. Welcome to ICANN83 CPH DNS Abuse Committee Update on June 9, 2025. During this opportunity the CPH has prepared a few areas to talk about and open up a conversation with the community, and just as a bit of context we have developed amendments to the registry agreements and the registrar retention agreements to add minimal obligations to respond to DNS abuse reports or actionable DNS abuse reports. Continuing that work and evolving the conversation

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

on DNS abuse and how to mitigate it, the CPH has prepared a few areas where we believe are worth of conversation. This is a starting point to start that discussion with the community and mature those ideas, in turn have input from the community and see how we can solve for this, including work on PDPs or other vehicles that we can use in order to effectuate those types of work.

Today we have an agenda here and we'll go into that in a bit. Can we go to the first slide please? Yes. What to expect today? Again, we're going to be discussing four topics. It's presented as potential policy questions that we want to work on. Why does the CPH believe it's worthy of discussion? Also, in other areas that we want to talk about, because we don't have all the answers, but we want to have this conversation with you, the community. I'll just take the opportunity to remind folks there are open seats. This is not a table reserved for the CPH, so if you want to come to the mic, please do now.

We're going to present four topics. Chris is going to help moderate that discussion. After this meeting what we want is to create a specific output for each of these topics. We're going to take the information that we've gathered today, create those documents, socialize it with the community, and use those tools in order to fit into the GNSO Council's small team discussions as they are identifying gaps and trying to find worthy topics for the next policy process.

Next slide, please. Housekeeping rules; rules of engagement. We're talking about here DNS abuse as defined in the ICANN contracts and in the ICANN remit, which is the five broad categories: phishing, malware distribution, botnet command/control, spam when it's used as a delivery mechanism, and last but not least, pharming. We want to engage in a collaborative and constructive conversation and we ask that we focus on each of the topics we are presenting. Again, each of the topics will have its own time. We are going to present that. We want to open to questions and some comment and to gather all the feedback that we can get in order to, again, create these helper documents where we can discuss what is the problem at hand. What's the rationale behind it? What are the things that we might need to address or not in future work?

On that point, we want to be as effective and we want to collect all your feedback as accurate as possible and don't want to miss, so we are asking for you to use the Q/A part, not the chat box because that gets sometimes mess with all the chats that are going back and forth, so let's use the Q/A part if you want to ask a specific question on the topic at the moment. Of course, you need to login to Zoom. We're going to be monitoring the queue. I'll give you a couple minutes to do that.

With that I think, can we go to the next slide, please? There you go. Now I will hand it to Chris, and eventually Luc and I will also intervene. Chris, over to you.

CHRIS DISSPAIN

Thank you very much, Dennis. Hello. Good afternoon, everybody. I'm Chris Disspain. I'm just going to, while you're all logging into Zoom so you can put your hands up and use the Q&A part, et cetera, I'm just going to go through these guiding principles. Number one Dennis has basically already covered, that we're dealing with the ICANN definition of DNS abuse.

The second guiding principle is that these ideas and thoughts need to be narrow in scope, short and constrained to solve a specific problem. If you remember, right at the very beginning of this whole thing, when we started doing the contract amendments, one of the things we talked about was dealing with the subsequent issues in small, bite size pieces to make sure that they were doable and could be solved relatively quickly.

The third guiding principle is the technology agnostic, so it avoids prescribing tools because tools can become obsolete over time, and the fourth guiding principle is that it's business model agnostic because it needs to work for all contracted parties, even if one framework, but adaptable to unique business realities.

With that, if I go to the next slide, thank you, think about while you're listening to the brief presentation on each of the ideas, think about the policy questions being described. You'll hear why the CPH believes the work might be beneficial and what are some of the areas to be addressed. Once that's gone through, once Luc or Dennis has gone through that for each of the four, we're going to

come back and ask you for comments, input, questions and so on. You can put your question in the Q&A box, you can raise your hand in the Zoom room if you would like to speak. If you're not at the table, you might be challenged with that, but you're welcome to come forward and use one of the microphones at the table so that everyone else can hear you.

With that, let's go to the next slide. This is the first of the four that we're going to discuss today, and Luc is going to take us through this. Luc.

LUC SEUFER Hello everyone. Yes, by pivot here for the non-Excel geek what we mean is taking a bird's eye view on the abuse, the DNS abuse report, so thanks to the contractual amendment, now the registrar, when they receive a DNS abuse report, they have a contractual obligation to investigate and to determine whether the report is actionable, and if it is, they will mitigate the abuse. The mitigation action will be different depending on the case. If the domain name is my compromised, the registrar will ask the registrant to fix the issue, but if it's malicious registration, the registrar will suspend the domain name. For those malicious cases, most registrars will look at the other domain names that are in the same customer account. For example, if you receive a phishing case with bank name 1TLD and you see that in the same account you have big name 2TLD, big name 3 and all—

CHRIS DISSPAIN Luc, you need to slow down slightly.

LUC SEUFER Oops, sorry.

CHIRS DISSPAIN Thanks.

LUC SEUFER Okay, so if you see that you have other phishing cases or maliciously registered domain names in the same account, you will suspend it, but right now, or the registrar will suspend it, but we have no obligation to do it under the contractual agreement or under any policy. The idea here is to require registrars to take a look at other domain names in the same user or the same reseller account or that share similar registration data, payment data, that are bought within the same order. The idea makes sense in principle, but the implementation really requires a lot of finesse and granularity because the policy will need to be narrowly scoped and the results will need to be scalable, and like you said before, Chris, adaptable to every business model.

CHRIS DISSPAIN Okay. That's the first of the four. Perhaps we could start by asking if anybody has any questions for clarification, anything that they

don't understand about what Luc's presented on the slide or anything that they'd like clarification on. This is going to be a very quick meeting. Okay. I'm going to take it that everyone understands. Now what I'd like to do is to take comments, questions, thoughts, ideas about how this might be approached and so on. Open floor. Ask anything. I'm being asked to remind you to use the Q&A part as well, but you're welcome, as I said, to use a microphone if you'd like to. Anyone? Afternoon tea will not be served, so take advantage of the time. Alan? My apologies, I didn't mean to laugh. Well, I did, but Alan, go ahead.

ALAN WOODS

Alan Woods for the record. Just one thing that occurs to me, and obviously this is wonderful and using the data that is there, I just would counsel some amount of caution when it comes to being prescriptive on what to share or what should be looked at because as soon as you start talking about that wonderful thing of personal data you're going to get into a position where perhaps is this is an enforceable policy or something from an ICANN point of view, that there may be a question of controllership, and that's just something that from past punch-drunkenness, that we will want to avoid like the plague because, again, they're directing you must use the data that you hold in order to pivot. I think you need to be careful with not making it too prescriptive, making it as open-ended as possible so that it's not necessarily you have to process personal data, but you use data that is available.

CHRIS DISSPAIN Can I ask a question for clarification? It seems to me to be slightly weird that we would be looking at a situation where we've got abuse and saying that we can't deal with it because it might be a breach of privacy.

ALAN WOODS No, no. I'm not saying it's a breach of privacy. It just gets much more complicated once you bring controllership and concepts with somebody directing you to process personal data in that sense. I would avoid that, directive to avoid if possible.

CHRIS DISSPAIN I have Volker and the Catherine. Who did I miss? And Owen.

VOLKER GREIMANN Thank you. Volker Greimann speaking for the record, if there is any. I like the idea, the general principle. I, however, am a bit worried about how this will look like in actual policy. It might be something that's better suited for recommendations for best practices, simply because of the business models. A customer account for a retail registrar is something different entirely than a customer account for a wholesale registrar. The data that we use for making such determination, and our registrar does already pivot in many cases and finds more domain names than those that are actually being reported, may very from case-to-case. To be prescriptive here on

the one hand risks not being encompassing enough. On the other hand, it might also risk telling the bad actors what to focus on and what to avoid when they don't want their domain names to be found. I'm actually in favor in having some for or shape of, I'm not saying obligation, but incentive to do more work than just taking down the individual domain name that has been reported. However, it needs to be closed in a way that it makes it workable and doesn't defeat its purpose.

CHRIS DISSPAIN Okay. Owen, my apologies, you and then Catherine.

OWEN SMIGELSKI Thanks Chris, this is Owen Smigelski from Namecheap. I like this idea. One of the reasons I do like it is because it's something that registrars are already doing. Similar to the DNS abuse amendments, those are things that a lot of registrars, especially the ones that participate in ICANN, were doing and we wanted to make sure that all registrars were doing that. I think this is one way to do that. I just would caution, I know we talked about if you look up the email address or customer account, the bad guys are listening to these conversations, so we need to be very cautious about giving them the blueprint on how to avoid these things that we're trying to solve. There may be some ambiguity specifically baked into this to say how you would do a check or whatever, and leave some discretion and latitude to a registrar based upon what information they may have, the business model, Volker has wholesale versus

Namecheap retail. We have access to two different things. Just allow us that flexibility to do that.

Then, I'm just going to disagree here with Volker. I don't think it's really useful to do an exercise and have best practices like this because best practices are what people who are the registrars in the room will do and it's not going to help with those that aren't here, where the abuse or concerns are, so I think we need to do, if anything does come forward out of any of these proposals they need to be binding and enforceable. Thanks.

CHRIS DISSPAIN Thanks Owen. Presumably the stuff you talked about in the beginning is the sort of stuff that if were to do a policy thing, that's when that would be dealt with, during that exercise. Thank you for that.

CATHERINE PALETTA Thanks, I wanted to go back. This is Catherine Paletta from Identity Digital. To Alan's point about data processing and controllership, I want to set that aside for contracted parties and the PDP. If ICANN is going to act as a controller under a policy they need to act like a controller and take on the responsibility of that. I think we've seen some hesitation, perhaps, of ICANN to do that and it's time for ICANN to step up if that's going to be something that they're worried about. I would say that's something they need to worry about. I don't think we, as the contracted parties, or even the

members of the PDP need to worry about ICANN's legal status as a controller. I don't think, Alan, you were necessarily saying that, so I don't think, but I want to be clear that to me that's an ICANN problem and if we want to do something about DNS abuse, we should do something and we shouldn't let that scare us away, which again, is not what Alan was suggesting either.

CHRIS DISSPAIN Thanks, Catherine. I'm very keen to hear what non-contracted parties might thing about this, if anyone is willing to come, either put a question or comment into the Q&A or come to the microphone. While we're waiting for that, I have a question as well, which is that I've heard discussions about this topic in alignment with a bulk registration issue. I'm not technically clever enough to answer this question myself, but is that just the other side of the same coin? Does that make sense? Sorry?

LUC SEUFER The one that's also addressing the bulk issue is the next one.

CHRIS DISSPAIN It's the next one, so we're going to deal with that.

LUC SEUFER Yeah.

CHRIS DISSPAIN Okay, super. Thanks very much. Did I see anyone else who wanted to come and talk about this particular issue? Mason, I saw you moving, so I'm assuming you're heading to a microphone. And Roger as well. Roger, do you want to go while Mason is… No, you're going to wait for Mason.

MASON COLE Hi, Mason Cole, chair of the BC. This is a great idea and this is actually something the BC and the CSG have advanced since the… Where were we last fall? Thank you, Istanbul. Chris, you were looking for some commentary from non-contracted parties. I think you'll find that non-contracted parties are very much in favor of this idea, would like to see it advanced. We'll do whatever we can to help contracted parties move this forward. Thank you.

CHRIS DISSPAIN Thanks Mason, that's great. Roger.

ROGER CARNEY Thanks, Chris. I guess I'm not going to add too much to this because I'm agreeing with almost everybody that's talked now, that says this is a good idea. Again, I think a lot of registrars do some of this. I'm not going to say they do all of this or anything like that, but I think that a lot of registrars have pieces of this, so I think it's not a stretch to add this. Again, though, I will caution on, I think Alan started it and it's gone through everyone now in some form, of being flexible here because I don't think you can prescribe exactly,

if you get it you have to look up their email and you have to look at their name. I think you have to be more flexible and I think, to Owen's point, I think it can be policy and I think it can be structured well enough that everybody's held to it. Thanks.

CHRIS DISSPAIN Thanks Roger. We can very easily talk ourselves out of doing this, as you said, by making sure that we make it so we pre-prescribe everything before we go in and start working on it, but I agree with you. Catherine, you were nodding?

CATHERINE PALETTA This is Catherine Paletta again, from Identity Digital. I wanted to go back to, Chris, your question about bulk registrations. Not to disagree with my esteemed colleague, Luc, but I think there is a bulk registration aspect to this. Hypothetically, again, not getting too prescriptive, I have a registrar. I don't have a registrar. ID has a registrar called name.com, and when they get a report if they're looking at a report for a domain name that follows maybe certain characteristics or all registered at the same time, they can pivot on that report and see that, wow, somebody registered 300 other domains that look pretty much the same and are registered all in the same account or registered at the same time. It avoids having to define bulk, which I think is really important. This is post hoc. We're not addressing bulk registrations maybe before or at the time they happen, because we know there's a lot of legitimate reasons to have bulk registrations, but we can address them after the fact

when they're found to be abusive, and I think this helps with that because instead of taking down one domain when 300 have been registered and are being used for the same phishing scheme, you can nuke all those 300. You don't have to wait for reports on those. Thanks.

CHRIS DISSPAIN Thanks Catherine. Dennis? Oh, four minutes, okay. Anyone else got anything? Yes, Volker.

VOLKER GREIMANN Yes. I'm not saying that we shouldn't do that, but we should be very careful about how to do that ultimately. This is going to be very difficult to document, for example. How do we prove that we pivoted? How would compliance address the concerns or allegations that we didn't pivot? If this becomes some kind of bureaucratic nightmare where we have to demonstrate for every abuse complaint that we did this, did this, did this, did this, then have to document that somehow, write that down so we don't forget it because we get hundreds of complaints a day, then we spend more time documenting and pivoting than actually fighting abuse complaints and I don't think that's something the community intends and that's not what we should spend our time on. Thank you.

CHRIS DISSPAIN Thanks Volker. Somebody else's hand was up. Theo? Theo's hand has gone down. Theo, do you want to say something?

THEO GEURTS Yeah, not really. I just noticed that some of my points where already covered, but when you talk about pivoting, looking up the domain in the database, it also touches upon bulk registration. It also touches upon possible trademark infringement. A couple of months ago we were flooded with TikTok shops and then in sequence, and we were looking at it and we're going, "This isn't real. These are fake web shops. Is it trademark infringement? Is it fake web shops?" It doesn't really matter, it's going down because it's hurtful to consumers everywhere. When you look at your database and you make all these, when you start digging into it, you can make all kind of connections there, be it name servers. If you have the ability to check a nature of is there some reseller unit using DDoS-Guard in Russia, the very notorious web hosting company, you can go, "What's happening there?" Having the ability to pivot and move on from there is vital for every registrar in my opinion, but I do agree with what Volker just said. We don't want to go into some kind of accountability nightmare where we just have to document all of this because that is quite impossible if you have a wide range of pivot capabilities. Good point, Volker. Thanks.

CHRIS DISSPAIN Thanks. We're going to move on to the next one. One final call for any more comments on pivoting. Nothing, okay. Luc, you're back up. Next slide please.

LUC SEUFER Okay. This one is stemming from the infernal reports on the bulk registration potential for abuse. Like Catherine said, bulk in terms of number of domain names is meaningless for how to qualify, to define, so what matters here is the functionality, the possibility for a reseller to register several names in an automated manner. We are looking here **[23:49 inaudible]**. The idea here is to strengthen the requirement for registrars offering a reseller program with an API or a similar tool for automated registration. It's not to impose a limit on the number of registrations, but having a gating system or gating measure to access the APIs, to have obligation on the reseller such as you can see on the slide, having a direct abuse point of contact and also having stricter reseller terms for the registrar having resellers. Again, this will also need a narrowly scoped PDP, which will be adaptable to every business model. Also, as you can see, we will need to amend again the RAA to include this new obligation if it's going to become something, a policy.

SARAH WYLD Sorry, may I ask a clarification question?

CHRIS DISSPAIN Yes, you may.

SARAH WYLD Thank you. This is Sarah Wyld. I just noticed that the question for discussion talks about an advisory, but then the potential value talks about updating the RAA. Are those two connected or different ideas? Thank you. I'm not wildly familiar with advisories.

LUC SEUFER It would be both, like we did for the previous amendment. We had an advisory and also the amendment of the agreement.

CHRIS DISSPAIN Thank you, Sarah, thank you Luc. Any other questions for clarification on this, before we move to talk about it? Everyone clear? Feels like it. Okay. Comments, questions, thoughts, input? I love it, I hate it, want to take it out for dinner? Yeah, Volker.

VOLKER GREIMANN Yeah, I think I like this. Part of the reason why is because we're already doing that ourselves and the community-wide approach on that could be helpful. Sometimes we miss something, sometimes other have great ideas. Being able to basically lay out the requirements of resellers with regard to abuse mitigation in a more official way also helps us perhaps showcasing what we're already doing to the outside world. Right now, these are internal or contractual phrases, but it it's a policy, there might be some benefit

to broadcasting our processes already to the world. It should not, however, be constricting in what we can do. We should always be able to go beyond.

CHRIS DISSPAIN Thank you, Volker. Roger?

ROGER CARNEY Thanks Chris, this is Roger. Yeah, I really like this. I don't know what we're calling it, a little pivot on this bulk idea, because we always had the problem with bulk being discussed and not really defined. When we were talking about it, we got to the point of saying even if we defined it as two, as Owen and Volker have just recently said, the bad guys are going to then stop at two and create another account, stop at two, and they're just going to create 10,000 accounts. I love the fact, how we've pivoted on this concept and got away from the bulk idea and got into maybe really where the issue is. Thanks.

CHRIS DISSPAIN Theo, I know your hand was up and it's gone down again. Do you want to chime in?

THEO GEURTS No, thanks.

CHRIS DISSPAIN Okay. Anyone else? Anyone from outside the CPH? Thoughts and comments? Owen.

OWEN SMIGELSKI Sure. I'll throw my hat in the ring here. Thanks. Owen Smigelski from Namecheap. I do like this as well, too. I think having those obligations, they should go down to resellers as well, too, but API, I know that might be a little bit questionable outside of that. But I think the ungated, unrestricted API access is a concern. Not API access itself, as cited in other places, but one specific type, and I think this could go very far in addressing concerns. There are some registrars that do allow this where there's a lot of abuse and I think this could go very far in helping to resolve that. Thanks.

CHRIS DISSPAIN Thank you. Anyone else? Last call. Okay. There seems to be general agreement about the first two not being bad ideas at all, so that's encouraging. That will take us to the next one, which is number three, and Dennis, this is for you.

DENNIS TAN Thank you. We are at the third idea, which is mitigation of batch registered domain names generated by a botnet algorithm. Just as a way of context, the botnet algorithms are these computer programs that generate a list of, potentially massive list of domain names with a corresponding activation date which botnet operators use to launch their attacks. For example, phishing

attacks. Today, by way of the registry agreement, registry operators and also registrars as well, we can deal with botnets when presented with actual evidence. The idea here is move that action from individual registries to have a uniform way, approach, so that overage operators can act on verifiable information. What we're suggesting is the role of a clearing house vetting, verifying, evaluating these lists of botnet domain names so that it can be distributed among registry operators and registry operators, with that actionable evidence, can act on those. In that way we can mitigate DGAs at scale. The other areas where we think we might need to explore is some things that we've seen doing these things for many years. What if, when an existing domain name is one of these DGAs and the domain name is registered, but the registry actions these domain names so that it can prevent use by the botnet operators. What's the available tools for registrars or registrants alike when they find themselves in that situation? That's in a gist the issue at hand. Should there be a clearing house role for an agent to vet, evaluate, distribute this information to all registry operators, and from that point registry operators do what they do now.

CHRIS DISSPAIN Thank you, Dennis. Once again, any questions for clarification on what any of that means? Anyone not clear or require a bit more information? We do, we have Theo. Theo?

THEO GEURTS

Yeah, thanks. Is there a lot of DGA? Yes. Is it always a botnet? I have seen very little evidence of that. The last really big botnet was in 2008 with Goldfinger. We all remember that if you are long enough in this space. The last time we were hit with a major botnet was almost a decade ago, Avalanche. If I read the reports from Spamhaus and other operators in the space, there is not much going on that we could classify as a botnet. If you want to operate a botnet, put it in the block chain. You can never take that botnet down. I think before we move really into this, I'm not opposed against a clearing house which would make our lives a lot easier if there would be any substantial evidence of botnets, I think we should really check. Are these botnets still as rampant as a decade ago? That would be my advice for this group. Thanks.

CHRIS DISSPAIN

Thank you very much. Rampant botnets. Okay. Anyone else? Any other comments and thoughts? Any questions? Yes, I've got Owen and Catherine. Yep.

OWEN SMIGELSKI

Thanks Chris. Owen Smigelski from Namecheap. I like this idea. I guess just a couple of things that we'd want to consider more as well is, how are these domain names going to be taken care of? I know sometimes when you get these botnets or other things like that, they want them sink-holed or held on for a certain or held on for a certain period of time. We need to make sure that ICANN considers who's doing that so it's not the registrar has to keep

paying the registry in perpetuity or something along those lines. I do like that. Also, I like it because it's work for the registries to do. All the other proposals seem to focus on the registrars, so it's good that you guys get to jump in and have the fun. Thanks.

CHRIS DISSPAIN Thanks, Owen. Catherine, then Sarah.

CATHERINE PALETTA Thanks. I am still Catherine Paletta from Identity Digital and I was wondering, not to call anybody out, but this is something that we're talking a lot about working with law enforcement and if there were perhaps any law enforcement in the room that had a reaction to this. I don't know what's going on in the GAC right now. They might all be in there, but maybe members of the PSWG, if you're in the room and you want to give us feedback or feedback later, at another time, that would also be great. Did I summon someone? A former law enforcement.

CHRIS DISSPAIN Ladies and gentleman, a pretend law enforcement, Chris Lewis-Evans.

CHRIS LEWIS-EVANS Thank you, Chris. I like this very much, as you might imagine from previous work, but I think one thing I like in how this is written is it's not focused on law enforcement agencies. Cybersecurity tend to be

a bit more technical than law enforcement. There's definitely none in the room, so that's fine, and they tend to be able to decode the DGA, find the DGA and support law enforcement to investigate it, but if this is action, it needs to include them as well. I think the cybersecurity side is really important in this. Yeah, I think that aspect's really important. There are some really good institutes. The Fraunhofer Institute is one that does a lot of work on DGAs, so having them involved in this I think is a good aspect. The one thing you might bump into is where there is an ongoing investigation. Some sort of clearing house might need to think about that as well, but generally very supportive. Thank you.

CHRIS DISSPAIN Thanks, Chris. I've got Sarah next.

SARAH WYLD Thank you, this is Sarah. I also like the idea. I just want to suggest, as the work continues there should be consideration of operations concerns around communication when action is taken. If a lot of domains suddenly disappear the registrar might be worried as to why that happened if they haven't been informed. Also, how to address false positives, which I think is an issue with reputation blocklists and this sounds a little similar to that. No? Not an issue? Great. Thank you.

CHRIS DISSPAIN Nick?

NICK WENBAN-SMITH Thanks very much, Nick Wenban-Smith, Nominet. In another role I chair the CTNSO's DNS abuse standing committee and when it comes to the DGA issue, I think it's very interesting for me to come into the GNSO room, but there are lots of CCTLDs as well and DGAs are agnostic as to whether it's a GTLD or a CCTLD. I suppose when you're asking for feedback, one thing that I would say is, can you create something such that likeminded CCTLDs could opt into it? I think a lot of them would opt into it voluntarily and that might be more effective across the whole ecosystem, and as Chris, you and I have talked about many times, when it comes to CCTLDs and GTLDs, there are lots of areas where we are TLDs and have a strong unity of interest in a solution which is customizable or scalable and applicable across the whole ecosystem. Thank you.

CHRIS DISSPAIN Thanks, Nick, and needless to say, I agree with you, and it gives me an opportunity to plug the… There's a joint CCNSO and registry stakeholder groups session on Wednesday I think, Wednesday afternoon, when the registries are all going to get together and talk about registry stuff, and that is a classic example of where there's a massive crossover and we should be talking more closely with each other. But Chris, you wanted to say something, I think.

CHRIS LEWIS-EVANS: Yeah, thanks. Just to double down on what Nick said, I think as Theo said, the last one was Avalanche. There was 400,000 domains, 200 TLDs. There was no difference between Gs and CCs. They don't care. A DGA is a DGA is a DGA. I think building in CCs along with this is really, really key. Thank you.

CHRIS DISSPAIN: Thanks, Chris. Dennis?

DENNIS TAN: Thank you. Yeah, and Avalanche, still going. Chris, I just wanted to… No, the other Chris. Yes. I just want to follow up on a remark that you said about considerations of current law enforcement investigations and that might be useful to understand because not every DGA has to be suspended. There are methods in which law enforcement or other agencies want to analyze the traffic and to notify big themes or try to find the actual infrastructure, not do the whack-a-mole thing with the individual domain names. Can you expand on that from your insights? Thank you.

CHRIS LEWIS-EVANS: Yeah, thanks, Dennis. Sink-holing is probably the biggest thing that happens with a DGA. The main purpose for that for law enforcement is to be able to identify victims and do some form of protective messaging. Normally a DGA is used for communication with infected machines and you tend to have lots and lots and lots of infected machines and law enforcement's role there is to try and

help clean up those infected machines, so to be able to sink-hole a domain rather than just suspend it is really key in actually tackling the harm that's being cause by the malware behind the botnet or the DGA.

CHRIS DISSPAIN: Okay. Any further questions or comments on this one before we move on to number four? Rod, welcome.

ROD RASMUSSEN: Thanks, Rod Rasmussen, CAPWG for this meeting, anti-phishing working group. DGA still exists. They're largely smaller scale these days but they affect multiple TLDs, but you don't see the big, giant, huge ones like we saw 10 years ago, but they're still there, which makes them a little more interesting in a way. I just want to point out they're also used for back-end communication between control servers as well, so not just sink-holing for looking at victim notification and cleanup, but also for trying to piece together the actual infrastructure is an important aspect of that. This is a topic area, I'm not as sanguine on this one, just the way it is, but I think the goal is right. There are a lot of stakeholders here and there are a lot of folks in the cybersecurity space that have business models built around sink-holing and providing data and information to their customers. If there was to be an effort launched here, it needs to have a wide net of people, stakeholders at the table talking about it. One of the things we run into in that space is, law enforcement calls it blue-on-blue, which basically means you've

got good actors, for a definition of good, that are interfering with each other because they're all trying to grab ahold of things. One thing I want to point is that most of this stuff, once you understand a DGA, the real thing is just making sure that they're blocked from registration during the time period that would be effective rather than suspension of existing stuff. Then you also have this, somebody mentioned false positives, and there's lots of false positives when you have DGAs that are based on common words and things like that. There's a whole lot of work that would have to be done there, plus just the organization of who would be entitled to sink-hole and do things like that once you determine that. There's a lot of work here. This is not a simple thing. Thanks.

CHRIS DISSPAIN Rod, if I could ask you a question, then. The chicken must be done. If we were going to do some policy work on this, getting that outside or expert into the work that we're doing, is that something we could start with SSAC and work outwards from there, or do we need to go somewhere else? How would you suggest we tackle that issue?

ROD RASMUSSEN Sure. I think within the SSAC there's plenty of people who have ties into that community and expertise in that area, and we're already here. I would think that there's some other organizations out there that have interest in this space that have done lots of work on this, lots of best practices and stuff as well. Again, if there's work to be

put together, some of the folks from SSAC can help you bring in, but I would bring in outside folks who don't show to ICANN meetings, because they don't necessarily understand the machinations of what goes on.

CHRIS DISSPAIN Thanks, Rod. I've got Volker and then Jody.

VOLKER GREIMANN Yes. Just as a word of caution, just because bad guys use DGAs doesn't mean that all DGAs are evil. I have learned a while ago that domains that were clearly DGA generated through our platform were actually legitimate. They were used for online marketing, domain parking, zero click parking, traffic redirection, all kinds of stuff that is not necessarily illegal, but they might be flagged by this as well. Therefore, we need to be very clear about what we mean by DGAs and that we want to control the use of DGAs only there, where it is malicious, not where it's not.

CHRIS DISSPAIN Thank you. Jody?

JODY KOLKER Thanks Chris. I'm just curious. Can you guys hear me all right?

CHRIS DISSPAIN Absolutely. Perfect.

JODY KOLKER

Okay. I just wanted to echo or summarize what people have been saying here, but what I see from an operational standpoint from this is actually a lot of work, just as Rod said. We need to decide if the registry or the registrar is going to sink-hole a domain, how it's going to be sink-holed, if the domain is going to actually be transferred to maybe another registrar where all aspects of that domain can be controlled by that one registrar, at least for GTLDs and maybe CCTLDs could do that, too. But I just want to caution everyone that there's a lot of operational work to be done here, and as Sarah said, there's a lot of communication that needs to be done between the registrant, the registrar and the registry. It's just a lot of work. Thanks.

CHRIS DISSPAIN

Thanks, Jody, point well made. I've got Catherine and then Greg.

CATHERINE PALETTA

Hi again, it's Catherine Paletta from ID. In going back to those starting principles or whatever Chris called them, I hadn't thought about, or if I had thought about it, I wouldn't have been knowledgeable enough in this space to know how complicated this is, is what I'm hearing. I'm wondering if what we're hearing indicates that this is not something that can necessarily be solved through this, while meeting those principles of tightly scoped and all of that. That is good to know going in, and maybe there's

something we can solve that maybe doesn't solve everything of this but makes a meaningful step that we can do that meets those tightly scoped principles. We'll look to the GNSO councilors and the GNSO small team to really look at that, but I think Rod, your expertise on this is really valuable because I was like, this seems easy. This seems like ICANN stands something up and that's doable, and I'm learning that it's not. I'm wondering. That should be something I think the GNSO small team certainly considers with this proposal because it sounds like it's not as maybe tightly scoped as we thought it was.

CHRIS DISSPAIN Thank you, Catherine. Chris wants to make a comment and then I'm going to go to Greg.

CHRIS LEWIS-EVANS I think it can be tightly scoped. I think there's a lot of definition and understanding that needs to go on first and SSAC might be a good first call. Can we write a paper on what are the correct actions to take for DGAs to properly mitigate them? I think once you have that understanding, that's when you can probably get that tightly scoped product. Without that understanding, yes, it is complicated, but spacing down what is a sink-hole, when to use it. When do you block the domains from being created? That understanding is needed before I think you can do this work.

CHRIS DISSPAIN Thanks. Rod, did you want to say something before I go to Greg?

ROD RASMUSSEN Just that I have no official ability to promise anything from the SSAC.

CHRIS DISSPAIN Thank you very much. We'll go to Jim in a minute, who has also got no ability, but will say something. Greg, you first, then Jim.

GREG DIBIASE Yeah, thanks. This is Greg DiBiase from Amazon. I was going to say something similar to Catherine. The first two are squarely within the ICANN policy development process. This is more complicated, has more external dependencies, I think, and it also seems like something that we can just do. I don't know if you need ICANN policy necessarily to start work on this, whereas the first two you're talking about obligations on registrars or contracted parties that the policy would actually need to change to make those effective. I see the first two more well suited for policy development, whereas this seems like a project that can be undertaken just in this community that we've built. These people right here. Then, down the road, maybe that work identifies what the policy change in question should be as this idea matures.

CHRIS DISSPAIN Like a study group type of thing. Jim, then Volker, then I'm moving on to the fourth.

JAMES GALVIN Thanks, Chris. James Galvin, SSAC liaison to the ICANN board, or Identity Digital, however you care to hear me speaking. I actually interpreted this suggestion differently than the way some of the discussion is going. I want to offer a question and tease this into two possible things here. I had assumed that, my interpretation in looking at this was that this was about the ability of all registries and registrars to be able to work with ICANN in managing the presence of a DGA and that that's what this was about. The existence of a DGA would have come probably from law enforcement or whatever mechanism it came from. It's out there. Let's put it on a list. ICANN already has processes for working with registries and registrars about dealing with DGAs, so it's a known quantity that's there and it's about documenting all those processes and making them known. That kind of thing, as opposed to identifying DGAs and doing that research and being in part, pulling all of that out and getting the names togethers. I had assumed that all that work would be done by the time it came here. I don't know that we have to answer that now, but that's two different questions in this policy. If we have an answer now, that'd be great, but otherwise I'd like that as a clarifying question for the work on this. Thanks.

DENNIS TAN

Quickly, to try to answer that question, maybe not, but for example, what Chris Lewis-Evans said before, Fraunhofer Institute does that work today in some way or fashion, so they can provide information. But how can we distribute that information across all registry operators uniformly? Not every single registry operator will be affected or implicated in that DGA because bad actors choose different liaisons and whatnot, but that would be the source in order to provide information. Does that answer your question in a way? I'm not saying Fraunhofer is the answer, but there are sources today that can provide that such.

JAMES GALVIN

Right, so I assume you're then suggesting that my first interpretation is the one that was planned. You're not suggesting trying to get up a research group in ICANN that goes and looks for these things and does it. Okay, thank you.

CHRIS DISSPAIN

John, before I got to Volker, do you want to say something?

JOHN

Where this has a similarity to some of the previous things you're talking about is this work is already happening. A lot of registries are already doing this. I've been involved in many of these, and yes, there is a lot of technical work beforehand to come with a well declared list of names, doing all the false positives, seeing what's resolving, seeing what's not resolving, seeing what's behind them.

All of that technical work needs to happen, but then there are a set of policy questions and implications when this comes to a registry or a registrar and they want to take action. Some of you may know that we have a process for enabling us to waive parts of the contracts and fees directly related to this and that exists. I wouldn't say it's a lot of work, but people have to do it every time they take one of these down. We did that because there are policy questions. Maybe it's not a small thing to deal with, but I think there are questions to be answered here that would make easier for everybody in this industry to understand how this works and to know what they can and can't do. So many times I've had the conversation when I've talked to somebody in industry. I'm often the person, I've worked with Chris and others in the past, that has to go to industry and says, "Here's this thing. Let me explain it to you. Let me explain the technology. Let me explain all the due diligence that's being put in place. Let me explain how this is all going to work," and then we get there but the policy doesn't let us do this or our contract doesn't let us do this. I think there's work to be done here. It may just not be the first PDP you want to take on.

CHRIS DISSPAIN Thanks, John. Volker?

VOLKER GREIMANN Yes. To add to that, probably not all of us are experts on this. We will most likely not be able to identify the registrations ourselves. Those registrations might not be malicious or active at the time

that we look at them. We might not have the right tools to assess whether a domain name that is registered through us is part of such a network, so we have to somehow rely on an external source that tells us this. Some of these have been registered across multiple providers, across multiple TLDs, so this is not something that any individual registrar or registry can tackle. This is something that will need an overarching framework of information that we will be able to rely on when we take action.

CHRIS DISSPAIN Thank you, and Sam, you get the last word on this.

SAM Thanks, Chris. Volker, I think that's very squarely the point of this, is that it leaves the identification in the hands of an expert group and it just facilitates the action across different registries in a way that is a bit more standardized and hopefully faster and therefore more effective. I think we're all circling back to that main point, but just figured I'd give Dennis and Chris a break.

CHRIS DISSPAIN Thank you. Okay, Dennis, back to the final one.

DENNIS TAN Yes, next slide. There you go. Last but not least, best practices for report phishing. Phishing reports, that's being one of the categories of DNS abuse in which when registrars mainly, but registries as

well, they are presented with an abuse report and it's actionable, meaning it has the proper evidence justifying the impersonation and also the intent to steal sensitive information, then it's acted upon and that there's some nuance about what mitigation action is chosen on a case-by-case basis depends on a high-level, whether it's a malicious registration or a compromised asset as in a hacked website or a hacked registrant account, whatnot. What we've **[55:48 inaudible]** has, when looking at phishing reports, what we see is there's still room for improvement. Just as recently we had a workshop in Seattle with the CSG looking at real examples of reports that are not actionable and we were going through the exercise of describing what is missing or what's not missing, why an alleged phishing report is not actually phishing. The CPH has put resources for the community to consume about how to report phishing to contracted parties so that it has the highest quality information and all the proper elements for it to aid in the investigation and any actions that follow. We frame this as a potential policy conversation, but maybe it's not a policy conversation at the end. The issue here at hand is how can we elevate these best practices so that reaches a critical mass, so that abuse reporters feeding those reports to contracted parties use these best practices in order to provide the evidence that is needed, in order to act upon those abuse reports. In that way reduce mitigation times, in that way reduce victimization. That's the issue at hand.

CHRIS DISSPAIN I'm guessing everyone pretty much understands that. Volker, did you have your hand up, or is that an old hand? You did. Over to you.

VOLKER GREIMANN I think it's an interesting point because it touches upon something that we've been trying for a long time, which is reporter education and it touches on something that we and other registrars are already considering, which is enforcing formats or enforcing proper reporting. This can take many different formats. Some registrars are doing web forms which you cannot complete unless you have provided all the information that is required and that the registrar will require to action that. Others might be chatbots or might be a certain format that has to be completed. If it's not complete, it will be auto-denied, so there are ways of channeling reports for registrars already. Not sure if we need a policy for that, but I think educating reporters on what we need for a report, phishing is one thing, I think is the way forward. Discussing this practices that we're already looking at as a community I think is very beneficial for us, even if it does not end up with a policy.

CHRIS DISSPAIN Thank you. Janos?

JANOS DRIENYOVSZKI Hi everyone. This is Janos Drienyovszki, co-chair of the publicity working group. I felt called out so I feel compelled to say something. This is the first time I see these ideas, so everything I say

is very preliminary and should be taken with a pinch of salt. I think that all of these ideas seem good and worth exploring, but to me, also, on our side, there's a lot of thinking and also in the GAC there's a lot of thinking of what potential PDP topics could be further discussed. I have to say, we also are exploring ideas which are more preemptive than reactive. To me these ideas, all of them seem rather reactive. Once an abuse has happened a report has come in. I'm not trying to diminish the importance of that, but we believe it would be also good to explore potential policy development topics that are a bit, happen before, at the registration phase, to create for example friction mandates, support registration going on and so on and so forth. I will leave it at that. I just wanted to comment that we welcome these ideas and definitely for further discussion, be we believe I think we could go even further. Thank you.

CHRIS DISSPAIN Thank you. Anyone else? Last call before we move on to next steps. No? Okay. Next slide. Next steps, which is you, Dennis, I think.

DENNIS TAN Thank you, Chris. Dennis Tan, again. Next steps, as I said at the outset of this session, the idea of these four topics is to continue maturing and evolving based on the feedback that we heard today. We want to create four specific district output documents that we can socialize with the community, get farther refined those documents and then provide those as tools for the GNSO council small team on DNS abuse. This is a start of the conversation. The

CPH has not just these four topics. We have a list of all the things that we also want to discuss internally before bringing back to the table for conversation, but we also want to hear your pain points, the community pain points. As a tradition, the CPH has hosted different groups on conversations. We want to extend that and try a different thing this time around, so we have set up a web form I order to receive your pain points, in order to create this repository of ideas that we can explore as we meet, whether inter-sessional-ly or different ICANN meetings. The URL of that web form is posted there, fightdnsabuse.how. We'll just ask basic information for you to share with us and we'll be in touch as and when we're ready to engage farther, whether clarifying questions or put that topic on the table in a session like this and start talking about that.

Our next meeting of course is going to be in ICANN84, so we look forward to have these four output documents here to talk about and potentially other ideas as well. With that, I turn it to Luc.

LUC SEUFER Next slide please. As you must know by now there is an initiative from the RSG, but it's a website under acidtool.com, and it allows you to identify for abuse reporter and any interested party, actually. You can identify the registrant, the registrar, the hosting provider, the main service provider. If you want any technical knowledge, you just enter the domain name and you get access to what is publicly available. We've operated a major update, so it's

version 2.2.1, so it looks good. It's faster. It's using RDAP, not WHOIS anymore, so go use it. It's still free.

CHRIS DISSPAIN Thanks, Luc. Thanks, Dennis. Owen, did you want to say something? Go ahead.

OWEN SMIGELSKI Yeah, I just wanted to chime in. I coordinate with the people who do the ACID tool updates. This is Owen Smigelski for the record. In addition, Luc mentioned it does RDAP instead of WHOIS. It actually still does WHOIS because ACID tool will also do CCTLDs as well, too, and if for whatever reason there's an RDAP failure, it will use WHOIS as a backup. You can get stuff from more than just GTLDs to the extent that it works with the CCTLDs as well, too. You may get not as much information, but one big thing I'd like to highlight is before you could not copy and paste. We had some issues with security on the form. You can now copy and paste the data out of there, which is one feedback that we had heard before that you had to manually write the data down, but now all that stuff is there. Thanks.

CHRIS DISSPAIN Thanks, Owen. So, we have about nine minutes left and we can finish. Before we do that, does anyone have anything else they would like to bring to the table, like to say? Any questions, comments? Paul?

PAUL MCGRADY Paul McGrady, just wanted to say thank you for a really terrific session. I feel like I'm a kid that came down the stairs and found all the presents under the tree and Santa got it right this year. Look forward to helping in any small way I can to—

CHRIS DISSPAIN You're going to be really upset when you discover all the boxes are empty.

PAUL MCGRADY Hey, but you know what? Three out of five presents are pretty good. Anyway, thank you. A lot of thought went into this. Looking forward to help in any small way I can to get this stuff across the finish line. Really terrific. Thank you.

CHRIS DISSPAIN Thanks, Paul. Jen?

JEN CHUNG Thanks, Chris. Jen Chung for the record, I guess now with a hat on for the council small team on DNS abuse lead. Thanks for the session. This has been really valuable discussion. It's good that CPH is teasing out some of the topics. Good to hear a lot of discussion from the rest of the community about it as well. Small team is on the eyes open, ears open mode for the Prague meeting, so this is

really… I see a lot of small team members in this room already listening. Great, thanks.

CHRIS DISSPAIN Thank you. Keith.

KEITH DRAZEK Thank you, Chris. Hi everybody, Keith Drazek with Verisign. I just want to take this opportunity to maybe reinforce and remind that when contracted parties undertook our negotiations with ICANN to affect the DNS abuse amendments in the registry and registrar accreditation agreements, we at that time underscored and acknowledged that that was just a first step. What you're seeing here today is our commitment, the commitment of the contracted parties to engage with the rest of the community and to support further policy work as warranted to continue to improve our capacity to mitigate DNS abuse. We really appreciate everybody's participation in this conversation. We look forward to continued dialogue on this. We fully expect that other parts of the community will bring other suggestions and other recommendations. All of that would feed into the GNSO small team, as Jennifer just mentioned, but I did just want to remind everybody that this is an ongoing process. We initiated that process with the bilateral contract amendments. We feel very proud of the work that we did in that regard, but we recognize that was just a first step, so looking forward to the next. Thanks, Chris.

CHRIS DISSPAIN Yes, thanks, Keith. Well said. Anyone else? Yes? Justine?

JUSTINE CHEW Thanks. Hi. This is Justine Chew speaking. Very pleased to be here again. I just want to do a little plug for At Large because I'm from the ALAC. We have a DNS abuse plenary on Thursday, the second session, in the At Large room. It's parallel to what's happening in this room. We want to have a conversation with the different parts of the community, and the panelists are made up of different parts of the community. Please do join us if you can spare the time. I believe it's South Hall Three, on the third floor. It's the At Large room, 10:45, second session on the Thursday. Thank you.

CHRIS DISSPAIN Thank you. Last call. Okay, with that, thanks very much indeed everybody, and see you in the next session. Take care.

[END OF TRANSCRIPTION]