ICANN75 | AGM – GNSO Council DNS Abuse Small Team Meeting
Saturday, September 17, 2022 – 13:15 to 14:30 KUL

UNIDENTIFIED FEMALE: Once again, welcome to everyone joining. Please log into Zoom. We will be utilizing the queue with raised hands. Make sure to use reactions "raise hand" when logging into Zoom. Please utilize your first and last name and we will begin the session in just a couple of minutes. Thank you.

MARK DATYSGELD: Thank you, everyone, for the patience. I will ask the meeting to be started.

UNIDENTIFIED FEMALE: Thank you, [Rick]. This session will now begin. Please start the recording.

DEVAN REED: Hello and welcome to the GNSO Council DNS Abuse Small Team Session. Please note that this session is being recorded and is governed by the ICANN Expected Standards of Behavior. During this session, questions or comments submitted in chat will be read aloud if put in the proper form as noted in the chat. If you would like to ask a question or make a comment verbally, please raise your hand.

When called upon, kindly unmute your microphone and take the floor. Please state your name for the record and speak clearly at another reasonable pace. Mute your microphone when you are done speaking.

This session includes automated real-time transcription. Please note this transcript is not official or authoritative. To view the real-time transcription, click on the Closed Caption button in the Zoom toolbar.

To ensure transparency of participation in ICANN's multi-stakeholder model, we ask that you sign into Zoom sessions using your full name. For example, a first and last name or surname. You may be removed from the session if you do not sign in using your full name.

With that, I hand the floor over to Paul McGrady and Mark Datysgeld.

MARK DATYSGELD: Thank you so much, Devan, for that introduction. Unfortunately, right now we are short on Paul. As we know, the arrival here in KL has been a little chaotic for everyone but hopefully he can join us over the course of the session.

Anyway, I would like to welcome the entire ICANN community. It's a pleasure to have you all here, everybody that can be in person and those who are joining us remotely.

The DNS Abuse small team from the GNSO Council promised we would have a report by ICANN75 but little did we know that our final meeting would be here with you, so we are kind of delivering on our promise. You just get to see the final pieces of the puzzle come together.

What we will do today is we have a session that's actually two parts. First we will go over very, very briefly on what has been our journey so far. You guys saw this who were on 74. But that will be very quick. Then we'll move into the actual progress that we made during these past few months. Finally, we'll get into a bit of a working session where we solve final comments and concerns which will allow us to finish our recommendation for the GNSO Council and hopefully start action on the next steps on this project which is pretty exciting.

Can we move to the progress update? Beautiful. So, if you remember, we were tasked with the effort of understanding if there were policy approaches to be taken, if any. So the team didn't set out to specifically arrive to the conclusion that there were policy solutions for the problem of DNS abuse.

And indeed you'll see that we found many different avenues to go to, and one problem that we had was the communities even remember during the pandemic time, we were discussing we need to tackle DNS abuse but what does that mean, right? We need to tackle it, we agree as a community but what does that actually look from a procedural standpoint? So that's kind of what we were trying to accomplish here. Next slide, please.

So, the SubPro PDP tasked us with this, and a small team was assembled because we thought that would be the most effective way to go about working on this matter. Like I said, there was a matter of do we define the problem? What is the actual problem? As you remember during the pandemic era, we discussed a lot of definitional problems

and the community was kind of stuck. We knew that we wanted to move forward but we didn't exactly know how. Next slide, please.

So, we reach out to you, to everyone. The different parties from ICANN, the different stakeholders received communication from us, as well as formal communication from our good friends from the DNS Abuse Institute who have been helping so much these efforts. And we made sure to reach out as much as we could to other stakeholders that we could not consult directly by these matters. So that was pretty good because we got an impression of where the community stood. And to be honest, what we found was positive. We had things in common. Yes, there are things we disagreed upon, but as a community, there are plenty of things that we agreed upon. That's pretty good.

So, going through that outreach took a little bit, but it helped us really understand what does abuse look like from the perspective of the community and where can it be actioned? What can we actually do? Next slide.

Here's an important slide. We went through all of the outreach. We didn't skimp on anything. We carefully combed through all of it as a group, multi-stakeholder group. And we found out a few things. Some of you may say, oh, that's obvious. Some of you may say this is novel. Let's go through them.

So, from our perspective, DNS abuse has a lifecycle. It's not something static. And depending on where it is in the chain of that lifecycle, different parties can act more or less on it. And by sort of creating a flow for this, hopefully we will help move discussions along in the sense.

Also, we are working with the idea that some issues could be resolved through conversation with contracted parties. There are some things that we are proposing and it's not … Let's use the word "propose" here because it is what it is. We are proposing that our friends from the CPH consider some minor amendments that would help us further this work, and normally this would be done through policy but we think that, for certain things, this could be expedited in this way. But again this is a suggestion that we are giving, and I will of course enter more deeply into what those suggestions are.

And finally, we classified the different efforts into buckets. What does that mean? It means that there is not a one-size-fits-all solution. As you remember, we were tasked to find if there's a policy solution. We think that yes, but we also think that there are other avenues that need to be considered and things that we could do as a community to mitigate this problem more effectively and those buckets serve that purpose.

We have a policy PDP bucket. We have one bucket that's about outreach and how we can effectively use our [tools]. And one is that suggestion that we are asking of the CPH for them to consider and potentially help advance this work in an expedited manner. Next slide, please.

I would also like to take the time to welcome my co-chair, Paul McGrady. Without him, this work would have been impossible. I don't know if you want to add a few words before we move ahead, Paul.

PAUL MCGRADY: Just a word of apology for rolling in seven minutes late. I had this on my calendar to start at 1:30, not 1:15. So, apologies, everyone. And Steve, thank you for the note.

MARK DATYSGELD: Great stuff. That's the benefits of having co-chairs after all, right? Paul has taken over for me, I've taken over for him. It's been good work. So, next slide, please.

Let's go to our lifecycle. Again, this is just conclusions that we have arrived at. This is not something that's set in stone or anything, but our suggestions will be based on this lifecycle, so I will go over them real quick together with you. Potentially we can even, if after I describe this lifecycle there are questions we can probably even have a small discussion about that.

So, phase zero is when the DNS abuse is still to happen or is about to happen, and this was reflected in comments we received on predictive algorithms and know your customer practices and different ways in which, ahead of time, you can even block the abuse from happening. So, what are the practices that we can implement to actually make sure that we don't even get to phase one and those exist. We need to talk about those.

Phase one is ensuring that the harmed parties know how and to whom complain about the report. So, this is something that we heard loud and clear from the CPH. They feel that sometimes the repots are incomplete, sometimes the reports are misguided, sent to the wrong place. And in phase one we want to make sure how do we engage not

only this community … Like we have been saying, we who are sitting here are the people who care. How do we engage the people who a) don't care or b) don't even know that ICANN exists. They're the ones getting harmed. They don't know how to go about processing this abuse. And if we are more effective about communicating that to them, then everybody wins. So that's phase one.

Phase two is the report should be well formed. This is something that we have seen advanced with DNSA Institute, the DNSAI NetBeacon project. But of course there are other products available, other initiatives. How do we get the right reporting?

Phase three is if you're well-positioned, if you're a contracted party or you're a host or somehow the message gets to the right people, action upon that.

And phase four, if this doesn't solve, we don't get it preemptively, we don't strike the iron while it's hot, we get it to compliance and we ask them "please help us." So those are the proposed phases.

Will this work linearly like that every time? Probably not. Most of the time, likely.

Very briefly, if anybody has a comment on that, this would be an opportunity to talk. And in case no, I'll move ahead. There's plenty of stuff ahead. Anybody on Zoom? No for now. If you have questions further, save it for later and we'll get to those. Next slide, please.

As you see, here are our buckets. Again, there's a question here. Do we do this sequentially or do we do this simultaneously? This is something

that we are I think close to working out. Maybe in today's meeting we'll get to discuss that a little more. We're leaning towards a certain direction but having the community's input will be helpful for that as well. How do we actually stage and sequence all of this? Next slide.

Here is the steak. For those of you who don't like steak, here's the tofu; I don't know. Here's the main plate. Let's call it that. These are our recommendations for the community.

We have made a lot of considerations, and those, let's say … These are the real recommendations, let's call them. This is what we are sending to Council and that we are asking that all of you from the community go to your stakeholders and start discussing seriously. This is our impression after researching this for a year of what we should be attempting.

So, recommendation number one. This pertains to malicious registrations. So, does the [beta merge during the online era]? We discussed a lot maliciously registered versus compromised. And while this was seen as somewhat novel at the time, I think that over the course of the past year or two years, these are really consolidated in terms of our perception of how this affects differently the community. A compromised domain name, it means that there was an interference in something that's already established. But a maliciously registered domain that only serves to carry malware, that only serves the purpose of phishing, that's probably something that's very much within our realm. It's technical. It's something that we can act upon based on the provision that we already have. So, if it is maliciously registered, we

know that for a fact. Why do we even let it live? That's the real question here.

And we want to suggest to the Council that this is discussed specifically. This is target. It's not a PDP just of DNS abuse, not boiling the ocean, not any of that. Let's discuss specifically what do we do with maliciously registered domains. How do we make sure those don't make it out at the gate? That's the policy development process we are proposing. That's the scope of it. It's narrow. It's supposed to be straightforward. And if you ask the group, I think that the suggestion is probably we don't let it happen. We create good practices for it to be mitigated. So this is the policy development bucket right now.

Recommendation number two. This is something that our friends from ALAC—and I point here to Justine who has been a starting member. We had the pleasure of having incredible team members who put in an astounding amount of work. Again, thank you all team members for working so hard. This is something that ALAC brought to our attention and Justine was a big champion of this.

What do we know about bulk registrations? Talking to our contracted party friends, we found out that not a lot. I mean, of course individually we know something. You know who your clients are and what they're doing, but as a community, we don't really. And this is a serious factor, especially when we are talking about command and control botnets. This is a serious factor. But even on phishing campaigns. This is something that's happening, and does it [tie] with the PDP? We don't think so. We think this is a conversation we need to have. This is something we need to talk about with the community, with the DNS

Abuse Institute, with the contracted parties, with everyone together. What do we know about bulk registrations? What are our practices? We need to start sharing this and we need to start working on what are the best practices as a community. We don't need a process for this. We just need as a community to understand what's going on and then potentially act up on it if there is anything to act upon. Next slide, please.

Recommendation number three. This feeds into valuing all the work that has been going on. Graeme just forwarded me their latest report on DNS abuse trends. It follows the pattern that we have been observing. DNS abuse is going down.

We have to say this certainly reflects upon the fact that we have been, as a community, on the ball about this. We have been on top of this. We have been discussing. We have been engaging. This is not something that we are just letting slide. We are really working together on this and we are trying to achieve something. The CPH is clearly reacting. We, the non-contracteds, are working on this with our clients, with the people. We are trying to have a conversation and this is clearly materializing.

So the question is what do we do so that when this is not a hot-button issue things continue to work well? This is a hot button issue now. We are seeing numbers go down. Great. How do we ensure that longer term things are still going well a few years down the road?

Because one of the things that this group discussed, we have this responsibility over DNS. We need to act upon it, because if we don't, other actors will come in and say that they can handle this better than

us and then we'll stop having that stewardship over it and this is something none of us want. So how do we ensure that this is a healthy environment?

And this goes to using the tools that we are developing as a community and educating people about them. Again, we are doing outreach. We are doing development. We need to keep talking. If the subject fades away and the next big thing comes along, this can just be shoved in some corner because we are making progress. How do we acknowledge that we are making progress and continue to do it?

And finally, we have the suggestions that we are talking about. So I won't drown you in legalese right now because it's not something we want to do on the first day of the meeting, but essentially we have some potential gaps in the RA/RAA and we think those could be tweaked. This is not something that's let's rewrite any contract. We are suggesting very small targeted and specific changes that could work on some of that language that's a little undefined. We have some language on those contracts as it pertains to DNS abuse that goes prompt. What is prompt? How do we ensure that not only the good actors but some of the actors who are not exactly in the room have some baseline to follow? Meaning the ones who are here are already doing, how do we make sure that everybody has those responsibilities?

And let me stress this very clearly. We are not recommending anything along the lines of changing the definition. The definition stays. It's technical abuse. It's right there. There's plenty of it. It is in the contract. We have discussed this extensively with compliance. The categories are there. Malware, phishing, pharming, spam as a vector for the others. So

we know what it is. The thing is how do we ensure everybody acts accordingly? And how do we go about this?

When we return to the Council now, we will bring this to a broader discussion and we will suggest the writing of a letter directly to our friends at the CPH for them to consider some changes and hopefully this will trigger a discussion that we can advance this as a community. We can advance this together, not in some sort of imposition but as findings that we have and that we hope we can advance together. Suggestions, again, being very clear. Next slide.

With that, hopefully we have made a succinct summary of our findings. Hopefully this has been useful. I would like to welcome any comments right now about what you have seen, and if there are no outstanding comments, then we will move ahead to a working session. I see Mason Cole has a hand up and I would like to welcome Mason to speak.

MASON COLE: Thank you very much, Mark. Mason Cole, Chair of the Business Constituency. First, I just want to, on behalf of the BC, I want to applaud the small group and all its work. There's been a significant amount of progress made toward mitigation of DNS abuse.

As you know, the BC has been very active on the issue of DNS abuse now for a couple of years at least. And part of our advocacy on abuse mitigation has been the idea that contracts could be updated to provide two things. One, a clear path for contracted parties to deal with mitigation of abuse and the other is to provide ICANN Compliance with tools to enforce against those who harbor against abuse.

I'm pleased to hear encouraging signs coming from contracted parties where I think we have some alignment on the ability to add some language to contracts on DNS abuse. I want to reassure everyone in the room and actually everybody here at ICANN75 that we're not interested in cracking open the contract and putting a bunch of amendments in there that would deal with all the pet issues inside of ICANN right now. We're more interested in really dealing with solely the idea of mitigation of DNS abuse.

So, during this meeting if there's an opportunity for us to align with contracted parties and others, we're very interested in having those conversations. I know we're all available to do so and there's going to be a lot of discussions about the RA and the RAA so we're looking forward to those discussions and we encourage alignment on this going forward because that's really a good way for us to make some progress. So, thank you, Mark.

MARK DATYSGELD: Thank you so much, Mason. It's very encouraging to hear from the community. I come from the business community but here I stand as the leader of this great group and hopefully that's exactly the path that we are taking. Very minimalistic. Nothing bloated and something that's helpful for everyone, literally every stakeholder. Everybody gets some use out of this.

MASON COLE: Thanks. I see Greg's hand next. Greg?

GREG DIBIASE: Yeah. Thanks, Mason. I just wanted to add a little more background on that from a contracted party perspective. Basically, what the report has in it and what the letter is going to identify, when we had asked Compliance some questions about CPS abuse, CPH abuse, some of their comments led some of the team members to think that there may be some ambiguity on what exactly compliance mechanisms are to have contracted parties mitigate abuse.

So, the letter that Mark referred to is basically identifying theses potential gaps. Are there gaps in the contract? Is this an issue with ICANN's interpretation of the current contract? These are just bringing these ideas to the contracted party house's attention and then they'll go from there.

But just as a reminder, any negotiation would be between ICANN and the contracted party house. I just want to make sure that is clear here.

PAUL MCGRADY: Thank you, Greg. Next up, I see Tomslin's hand. Tomslin?

TOMSLIN SAMME-NLAR: Thanks, Paul. The question I had was regarding the report mentioned that he just got. I was curious to know if the report, as it says that the abuse is going down. Does it say why? I'm just wondering, could some of the reasons potentially make some of these recommendations unnecessary?

MARK DATYSGELD: So, I'm posting this on chat. I'll be honest in saying that I only managed to skim it. I had been traveling the past few days. But I posted it on chat, and in case Graeme has anything to add about it, please add yourself to the queue, Graeme. Would you like to answer directly so that we create a bridge? Would you be ready to do that? I will hand it over to Graeme.

GRAEME BUNTON: Good afternoon, everybody. I'm Graeme Bunton. I'm the Executive Director of the DNS Abuse Institute. We published our first report 1:00 PM Eastern time, 1:00 AM last night, where we're trying to measure DNS abuse across the ecosystem. There's a good blog post on the DNS Abuse Institute website. And please check the chat.

We're not doing a lot of editorializing about what is going on. It's very early in that data. We really only published three months. So I think it's just too early to speculate about why DNS abuse is going up or down, something like that. So I don't think that I can answer that question really.

And a note about the data that we're using is that we're really optimizing for accuracy, so having a sense of overall trends is going to be harder than really understanding what's happening at the registry or registrar layer. That data will be coming, hopefully around November. But myself and Rowena—wave your hand, Rowena. Rowena is really responsible for this project at the institute. So we're here all week if people want to talk about that report. Happy to do so. Thanks.

PAUL MCGRADY: Thanks, Graeme. Mason, I see your hand is back. Did you want to reply to something?

MASON COLE: Yeah. If I may, I just wanted to follow-up on what Greg said. Greg, thank you for the comment. It's quite unnecessary to remind everybody, or at least the BC, that it would be only contracted parties and ICANN in the room.

This goes back to when I was Chair of the Registrars years ago we had the same situation. We're very aware of the protocol in terms of how this would be carried out.

What we're looking for during this session and during the meeting is alignment where we can align with the BC and others with the idea that there's an opportunity to improve contracts in a way that would mitigate abuse and that's really it. That's our only agenda. I just want to be clear about that. All right. Thank you.

PAUL MCGRADY: Thanks, Mason. Greg, is that an old hand?

GREG DIBIASE: Yes.

PAUL MCGRADY: All right. Just to address, I've not read the report or the reports to come but we all hope DNS abuse is going down, right? That's terrific. You'll see on one of our earlier slides when we talked about the policy development process, the idea between that one, it was sort of sequenced to allow some of the other things to move forward to see if that kind of PDP is even necessary, if more tools are necessary.

So we hope that some of these recommendations become obsolete because the community solved it themselves. That would be terrific.

Next up is Steve DelBianco. Hi, Steve.

STEVE DELBIANCO: Thank you, Paul. Graeme, I've only just scanned it briefly. I would love to see declining trends. But something I've asked you about before is whether it's really valid to report the number of unique domains from which abuse occurs as opposed to the number of instances of abuse regardless of where they originated. I understand it might be just difficult to get the data but I'd love your perspective on whether that would be the more relevant measure and why it is we can't use it instead of the unique domains from which they originate. Thanks, Graeme.

GRAEME BUNTON: May I respond? Thank you. So, from that blog post, there's a link to an actual published report which includes our methodology document which is very thorough because we partnered in this project with Maciej Korczynski from the University of Grenoble in France, and our

ask for him was very hands off. Measure abuse in the most robust, academically rigorous way that you could. Please and thank you. Then give us that data and we'll present it to the community. So that's where we are. And that methodology document is very academically robust. Make sure you've had some coffee before you read it.

But a key piece of that is what I think you're asking for, which is we are measuring by the unique domain name. We're not measuring by the multitude of URLs.

PAUL MCGRADY: Thanks, Graeme. I think our queue is empty. Am I missing any hands? Go ahead, Mike.

MICHAEL PALAGE: Thank you for saving me from logging into Zoom. I guess one of the things that I've noticed in 20-plus years of ICANN is sometimes things tend to be siloed. And some of the comments that were talked about earlier about choosing only to look at malicious domain names, malicious as opposed to compromised, and then there was the reported reference of KYC or KYB, knowing the registrant.

What's interesting is in the earlier session here today in this same room about accuracy, there was discussions and there was a split within the registrars that talked about when something is registered through a privacy-proxy and not knowing who that registrant is. So why was that decision made on malicious versus compromised?

And let me just give you one specific question which has me scratching my head. In the accuracy group, when we were talking about surveying, how we could potentially survey, the question was made: why not look at surveying the malicious domain names or the names that show up in DAAR to find out whether those domain names have accurate information? And there was incredible pushback from the contracting parties.

So I'm just trying to understand why the contracting parties were so adverse in a separate working group to get to this underlying information, yet they seem to have just coalesced around this bifurcation here. I don't understand it, and if you can shed some light, I would greatly appreciate it.

MARK DATYSGELD: Thank you very much for the comment. As one of the co-chairs, I will take this on. I'm evidently not a member of the Contracted Party House; I'm a member of the Business Constituency. So I will speak for the group right here and I welcome any group member who would like to pitch in to stop me or add to that.

What I feel is during the small team effort of DNS abuse, we were looking at a very specific interpretation which is what the community gave us. So we gathered feedback from the entire community and we were trying to condense what does the community think about these issues and how can we handle it in the best way possible? That was literally the way that we were dealing with this.

In that specific case, in trying to find the commonalities, we had two options. We can open the PDP on DNS abuse and that's another seven years of our lives. That's an option. It really is. It was on the table. Or we can look into where is it hitting the hardest? Where are opinions converging in some way? And we can actually get this focused, tight, and expedited like we have been saying for years now that we want PDPs to be … We don't want again those PDPs that never end and everybody gets frustrated. It burns out people.

So we are trying to work with what the community gave us and what seemed the clearest. In this case, from multiple parties, what we heard was the moment you talk about compromised you are not talking about the contracted parties anymore, per se, you are talking about a constellation of actors that may or may not be involved in it. How do we action a hosting provider from ICANN? That's a question I have. How do we action a hosting provider from ICANN? We don't actually talk to them. Of course the ones that are within the contracted parties that we have, sure. But what about the others? We don't have that kind of communication. ICANN is a silo in relation to the rest of the tech community. So maybe that's an issue to be tackled. But what can we immediately address?

What we can immediately address is the things that are totally within our control, which is registering domain names. So that was kind of the consensus. It may not be the best answer in the planet but it is an answer that is founded on things that are solid.

So, with that, I see that Greg has a hand up. And since he is a group member, I'm sorry for the people in the queue, but I'll give him the opportunity to pitch in.

GREG DIBIASE: Yeah. I think echoing a lot of what Mark said. We got a lot of comments not just from contracted parties but from all around the community that they didn't want an open-ended PDP. If there was a PDP, it should be tightly scoped and I guess efficient would be another word. So focusing on a maliciously registered botnet, that's a very concreate thing to focus on and try to make progress. So that was in response to feedback we got generally from the various ACs and SGs we talked to.

MICHAEL PALAGE So again, I applaud the work that the small team has done. Just a word of caution. And Greg, you had talked about this earlier when you made the reminder that there is a picket fence and the contracted parties have to agree. There's two ways changes to those contrasts could happen. Either the parties agree to make the change or consensus policy.

As we know, implementing consensus policy has basically stopped in ICANN. It ceases to exist. And what I'm concerned about here is if policy development only proceeds based upon when the contracting parties have agreed or pre-ordained what that change is and then we just use the rest of the community to rubberstamp it, that is inconsistent with the multi-stakeholder model that I've spent 23 years trying to protect.

Again, not trying to distract. I am just trying to urge caution on that slippery slope and how it could potentially threaten the multi-stakeholder model. Thank you.

MARK DATYSGELD: Thank you very much for the input. I'll give final comments to that in saying that one thing that I think that we have been careful about is lining up the Council around this, letting people know, getting the people together in the room, and we intend to keep that going.

The Council right now is pretty united. We are a pretty consistent group. We are really working hard on this and we all care very much about this, and hopefully we will keep doing the best that we can to move this forward, so hopefully you have to put a little trust in us which is hard to do. But at the same time, I can say that we are trying very, very hard to get this going.

PAUL MCGRADY: All right. Next up, we have Reg.

REG LEVY: Thanks. This is Reg Levy from Tucows and I wanted to go back to Graeme's answer to Steve's question about why focus on domain names specifically instead of the full number of URLs that might be used on a particular domain.

I know what my answer might be to that because there's only one mitigation that can occur, but I was wondering if Graeme had a different answer to why look at domain names specifically rather than URLs.

PAUL MCGRADY: Go ahead, Graeme. Thank you.

GRAEME BUNTON: Thank you. Hey, Reg. Sorry you're not here. It's nice to see you on screen, though. I think your answer is the correct one. The tools that registrars have at their disposal to mitigate abuse is at the domain name level. You will sometimes see even in compromised, sometimes malicious, where there are … I think the record that we saw in our data was 70,000 unique URLs associated with a single domain name. Counting 70,000 things of abuse isn't particularly useful if there's only a single place for mitigation, so that's really why we're focused on the domain name. Hopefully, that's helpful.

PAUL MCGRADY: Thank you, Graeme. Next up we have Werner.

WERNER STAUB: Werner Staub from CORE Association. When I hear that DNS abuse is going down I'm of course worried because that is not what I see personally. When I look at the DNS abuse, the BC, professionally as a registrar and registry almost see nothing. But when I see what happens

to friends, when I see stuff that is being sent to me, I see obviously there's a lot.

And then I see moreover that the domain names I discovered maybe a year ago that are still around. They were used for major abuse campaigns. They haven't been taken down. So, why?

Maybe one thing that we should ask ourselves is how much technical progress the abusers are making in remaining undetected? And this is probably the reason why we're seeing DNS abuse by the measurements that we've been looking at going down.

A "good" organization involved in DNS abuse is of course trying to save their assets. So what are they going to do? They're going to use each individual domain that they control only sparingly. A given campaign is going to be spread across many domains. And most importantly, they're not going to tell the same thing to every requestor on the same domain their URL. Yes, even if the same URL is submitted to [inaudible] visit by a different person from a different context, they will not see the same thing.

In order to remain undetected, the abusers know that they have to be sure that they're not going to be seen by the probes. So the best thing is don't put the malicious payload when the probe is visiting you. That's very easy. You have all kinds of targeting information that they have used. Typically the domain that I've seen being abused was used typically in a WhatsApp attack or instant messages or on YouTube or whatever. It is redirected two or three times until the payload is delivered, and in most cases, people like ourselves will not see the

payload because we have been detected by those systems as not being vulnerable. So they keep their powder dry when non-vulnerable people are involved. They know how to present the information only to the people vulnerable and only to the people who are going to be totally unable to react.

MARK DATYSGELD: Thank you, Werner. That's actually very on point. This is something that we have been discussing within the group. That is the question. How do we remain relevant? It's a real question and it's part of why our scope is so narrow, because we have arrived at a conclusion by uniting all of us together every week, each from a stakeholder group, we learned so much that we didn't know individually which leads me to the understanding that we simply don't talk enough.

Yeah, we have this fight in PDPs and we have our things and we have our mailing list, but we are simply not doing information sharing. We are not working cohesively. We are not working as a community on an issue that affects us all.

When I decided to be co-chair of this group, it is actually because what you said. I see people around me, small businesses, getting screwed over and I wonder, I'm part of this global community; we should be doing better. We are literally not doing enough.

So yeah it is a concern that I actively share, and to be honest with you, I don't want this to be the end. I don't know what form this will take but we will need to start a conversation, an ongoing one where we take accountability over this thing that has been given to us, especially after

the IANA transition. We can't just pretend like it's not a thing. It is a thing. Thank you.

PAUL MCGRADY: All right. That's the end of the queue as far as I can see, so I'll do a last call on that. Steve, go ahead.

STEVE DELBIANCO: Thank you, Paul. Steve DelBianco with the BC. I put this in the chat because, Graeme, when I said the number of instances was more interesting than the number of unique domains, you and Reg have clarified that one could perhaps measure the number of unique URLs that originated, and yet that stops short of what it was I was asking about.

I think that if the folks in the room believe we should only measure statistics at the level at which we can affect behavior, I would say that that's valid, that it isn't dispositive of needing to know the number of instances. The metaphor I would suggest is if we wanted to measure whether instances of bad driving, dangerous driving, was going up or down, we would want to measure the number of instances of dangerous driving, not just count the number of bad drivers and suggest that if there's fewer bad drivers that must mean that there's fewer instances because it isn't the case.

This is not a gotcha in any way. It was a genuine inquiry about whether the data would support a conclusion on whether the instances of abuse are going up or down, and if the data doesn't support getting there,

then we should say that. But we shouldn't conclude that we're counting unique domains because that's the only appropriate thing to count since that's where we can apply pressure. That's a different consideration. Thank you.

PAUL MCGRADY: Graeme, would you like to respond?

GRAEME BUNTON: Yeah. Briefly if I may. Steve, I apologize. I think I misunderstood what you were coming at earlier. Broadly speaking, I don't think counting either URLs or domain names is a great way of getting at harm, which I think is what you're actually looking into. Boy, I spend all day on this every day, thinking about these sorts of problems and I've never really come across even a ballpark way of translating from domains or URLs to actually impact some people which is really what we're trying to prevent at the end of the day.

So, boy, people have interesting ideas for that. Happy to hear them. I'm not convinced that measuring URLs is going to get us there either, especially when you can spin up essentially an unlimited number of URLs, whereas the domain name or counting unique domain names is a bit more concrete and it's where the action can take place.

So, what we're trying to do at the institute is help the industry combat something. So, for us it's about driving action at that level rather than understanding the potential harm, so I think it depends on what you're trying to do.

If you're trying to get a sense of the global harm, maybe URLs is a better place. If you're trying to come at a problem and see what can we do as an industry, I think URLs are a better way to come at it. Thank you.

STEVE DELBIANCO: Paul, can I follow-up really quickly? I appreciate it. Thank you. Graeme, I came back to this point just because Werner raised his concern. Werner thought he heard somebody say that DNS abuse is declining and to let him counter that based on experience and I defended what I heard from you because I don't believe you ever said DNS abuse is declining. All you said is the data showed that the number of unique domains from which originates is going down. That's good but it isn't the same thing as saying that the amount of abuse is down. Thank you.

MARK DATYSGELD: Thank you very much. I actually follow up on that by saying what we know from ICANN data and what we are seeing from the DNSAI … Everything uses different measures and I would say that what's happening is we are seeing things happen. We are seeing progress of some sort in some way, and the objective of this small team has been very clear from the start and it will continue to be to its end, which is we need to do things and we need to act instead of workshopping the perfect solution that will solve every issue on the planet. So let's keep developing metrics and let's keep advancing. Our objective, when this becomes a PDP, when this becomes a standing committee or whatever it becomes will continue to be this. Let's keep advancing the discussion,

finding your metrics and working as a community, no matter what happens. This will be it.

So this kind of exchange, perfectly valid. It is within the scope of what we want to do but it's not our goal. Our goal is how do we actually do something instead of spending the two-plus years we spent going "oh, I need this, I need that." Yeah, yeah, yeah. We all have different points. We want different things. There is more things we can accomplish as a community like generating better data, like discussing, making small amendments to contracts that actually force people who are not in the room to do something. That's all things that, in some way, will help move this forward and that's the objective of the group. Anything that goes much beyond that, it's not within our scope and we promised the community something. We will deliver a tightly scoped, small, strategic impression on DNS abuse and that's what we'll deliver.

Further work might be necessary but we are delivering pretty much what we set out to deliver.

PAUL MCRADY: Thanks, Mark. Thomas is up next. Then if anybody would like to get in the queue, now is your chance. And when Thomas and anybody else who gets in the queue is done, I'm going to make a brief little statement myself. Thanks. Thomas, go ahead.

THOMAS RICKERT: Thanks very much, Paul. Hi, everyone. I think this is an excellent discussion and I think it also shows the dilemma that we're in, that

different groups are producing different statistics and explain things differently, and if we count by domain name and others count by URI, it makes ICANN look like we're [bluffing] the issue which I think wouldn't do the problem justice, which certainly exists.

So maybe, as our work progresses, one of the outcomes of our group can also be that we evangelize more about terminology and how we talk about the problem.

On substance, I suggested that we include language in our findings which the group agreed to include there, that we are only dealing with a small portion of the thing but it's an issue of an entire ecosystem of Internet infrastructure providers that need to work together, and therefore the expectations in terms of what ICANN or the contracted parties can do should be managed because they're in fact quite limited.

I think that the discussion between Reg and Graeme was a very good one, particularly showing the difference between URI or domain level. For contracted parties, there is only a binary choice to be made. They can switch of a domain name or keep it alive, and therefore it doesn't matter whether it's 5000 URIs that are being used for a campaign. It's one domain name and therefore I think it's appropriate for contracted parties or ICANN, for that matter, to count by domain names.

On the other hand, if you have 5000 domain names pointing to one website for the ISP, it's one report. So we have different words that count differently and I think that maybe my concluding thoughts or my takeaway message is that we need to be very clear on who talks about what—and ideally we would just talk about campaigns.

So if there is one campaign by a group of criminals that is including 5000 domain names and 500 different websites, it should be one problem that should be solved by various measures. The one receiving the report should take action. They should probably notify their colleague registrars that also have domain names under management that are involved in that and then try to shut down the entire campaign.

PAUL MCGRADY: Thanks, Thomas. Last call. I mean it this time. Last call. Well, I think we've come a long way. Two years ago, we couldn't even agree on definitions to sit at the same table. Now we have a room full and we're discussing how to measure harms. We're talking about policy development versus informal community activity to try to fix this problem. Everyone seems to be at the table now. We're seeing organizations like Graeme's that are leading in this area and not being paid by Org to do so. Right?

So the ice jam on DNS abuse has thawed and I'm excited to see what the community accomplishes in the next several months and we're excited to deliver this report to Council hopefully very soon and we are looking forward to a lot of tough questions from our fellow councilors who may have a different view on some of these things when the letter is delivered.

But I just think today's discussion is an excellent example of how the entire tone around DNS abuse mitigation is changed just in the last couple of years. I'd like to thank everybody in the room who

participated and those back home who took the time to join and to communicate as well. Thank you.

MARK DATYSGELD: Thank you for that, Paul. We have a working session after this. But before we wrap up this session, thank you to everyone from the community. People have been—especially our group members, you have been incredibly civil. This group has been incredible. We just work, work, work, and it's all thanks to your efforts. Thank you very much for this group and thanks for the community for giving us such good material to work with. It's been a pleasure doing this. Hopefully as this work advances we'll have the pleasure of continuing to do these actions and this will continue going ahead. So, thank you so much. I will draw to a close the first phase. This is the exposition phase. You'll hear more from us very soon as we deliver this report to the council. Cancun is a long time away. We'll certainly be discussing that over there.

But before that will go to Council, we will get to discuss this as a community and we remain open to talking to you. We don't have to be in the room doing this. So when the report comes out, please make sure to reach to your representative from the small team, to me, to Paul. Talk to us. We want to continue working as a community and pushing this ahead as fast as we can and in the best way possible.

So I will draw this part to a close. Anybody who doesn't want to see the working session, please feel free to join other engagements and we will move to the working part of the meeting for the next 17 minutes and change.

So, very few points to open. I would say four. And the first one seems to be simple, at least in my simplistic mind. It is something that we have discussed in the past. I think I'm just looking towards the small team now for us to give a final okay to this.

As you remember, Justine proposed that we [add] that being in one bucket doesn't mean it can't be on the others. I think that this has been reflected in the document. I just want to make sure that we want this in the executive summary. If any group member doesn't feel that that's the best way to go about it, please raise a hand now. Otherwise, we will approve this change and we will go with that.

I see Marika has her hand up. Please. Or [inaudible].

MARIKA KONINGS: Yeah. Thanks, Mark. Just a question because I think Justine had put in here, as suggested on page seven, second to last paragraph. But I actually went down to page seven and there doesn't seem to be language in there so I just wanted to confirm with Justine if she's suggesting that that language should be inserted there or if she had made an edit there and it's just not visible. I was just looking for a clarification on that, if Justine is around.

MARK DATYSGELD: Can you clarify for us, Justine? I saw her. Sounds good. Can we at least change on the first part. I think that on the intro we can consolidate that, and Marika, if you could make a note about the follow-up page, that would be super good. But we can at least solve this first instance of

the issue. Then we can look at page seven when we have Justine available.

So, with that, we move to Greg's comment. Do we want to add the idea that this could actually be three PDPs focused on each type of abuse individually, as outlined by the DNSAI? To which Justine replied, "Perhaps we could say tightly scoped policy developments without enumerating how many."

Greg, I wonder if you want to discuss this a little bit, so that we give this a final body.

GREG DIBIASE: I don't think we need … I think Justine's language makes sense. I just wanted to open up the possibility that it's not a single one. I think Justine's suggested language captures that.

MARK DATYSGELD: Thank you, Greg. Does any team member think that we have better language? I like personally Justine's language but does anybody feel that there could be any added to this, this would be a great time to raise your hand or propose alternative language right now.

With no hands up, let's … Oh, Marika, please.

MARIKA KONINGS: I just note—and I don't know if Justine is referring to that because it already says "tightly scoped PDP" just above. I highlighted that. But we can obviously look at if that needs to be repeated on page seven or in

point four. But I think that's how we've already been referring to it. But we can double check if that language also appears in the other places.

PAUL MCGRADY: Thanks, Marika. We've got the word "this" though, which makes it singular. So we'll just have to make sure that we search out the singularities and eliminate them. Thanks.

MARK DATYSGELD: Yeah, can we do that? Yeah, go for it.

STEVE CHAN: Thanks, Mark. This is Steve from staff. I think there's a little bit of a nuance in the way that Justine phrased it. She said tightly scoped policy development rather than PDP specifically. So if you actually take out the PDP and call it policy development, maybe that actually provides some of that flexibility. Thanks.

MARK DATYSGELD: Yeah. That's kind of the angle that I was looking at, so that PDP meant something so specific, but policy development, it can encompass those extra elements. This is what I was looking towards. Thank you for the [hot] editing, Marika. That's looking good as it is. Yes. Policy development. we don't focus on PDP, because then we give the Council the flexibility to look at this from whatever angle they find most suitable. Does anybody have additional comments on this language or are we good?

Okay, I'll call this a victory. Every small victory counts, right, Paul?

PAUL MCGRADY: Every line of text is declared a victory.

MARK DATYSGELD: It's what we were saying in last week's meeting. If we start working like the GAC and fight over words, that means that we are actually winning because we're not fighting over big context.

So we have Sebastien's comment. I don't know if he is online with us. Seb, can you express whether you're there?

SEBASTIEN DUCOS: Hi, Mark. I certainly am.

MARK DATYSGELD: Thank you, man. Sebastien has also been working super hard with the rest of the team. Would you like to comment on this particular point, Seb?

SEBASTIEN DUCOS: Yeah. I just wanted to add the Registries Stakeholder Group, no offense or anything like that to Graeme and the DNSAI and all the great work that they do but I just wanted to make sure that the Registries Stakeholder Group was represented as the DNSAI doesn't represent us formally.

MARK DATYSGELD: That seems like a reasonable change. Does anybody in the group feel we shouldn't implement this change or are we good on this one? It seems fair, right? I think it's what we meant. We just didn't write it super properly.

GRAEME BUNTON: We definitely don't try and represent any particular stakeholder group or interest other than our own. Thanks.

MARK DATYSGELD: Thank you, Graeme. You guys may see the DNSAI over represented here but it's because they wrote us the longest letter in the planet. Thanks, Graeme. It took like six meetings to go through it—no offense. Thank you, buddy. That was great. But for real, DNSAI just provided so much material for us to work with, so if it looks like they're over-represented here it is because they really put in a lot of work to substantiate the work and I can't thank them enough. Like I said, we [inaudible] the outreach from the community with the output that they gave us. This is actually pretty good that we got that much from them.

We have an outstanding issue on page 14, which is a question from Sebastien that goes, "Can we verify the quote? There is an apostrophe missing." Is that an apostrophe? Is that what it's called? And the sentence ends on an open [inaudible], which Greg answered … Greg, can you clarify this one for us?

GREG DIBIASE: So, I was just going back and finishing. The quote seems to stop midway through, so I just posted what was from Compliance's response. I don't know if someone was looking for a different quote, but I just posted a quote that had the first half of that.

MARK DATYSGELD: Sebastien, can you relay to us … Marika wants to speak first and then Sebastien.

MARIKA KONINGS: Thanks. Just to clarify, actually, the quote that Sebastien has highlighted was just missing indeed the apostrophe. The one that Greg is referring to is actually the one just above. So it's the one that starts with "The RAA does not require registrars to take any specific actions." I think the suggestion is to maybe add that second sentence there, not to the sentence that Sebastien flagged. We've already added the apostrophe, so that should be fine. So just wanted to avoid confusion over that.

GREG DIBIASE: Sorry. In that case, I think you could just disregard my comment because I think that first quote captures the gist of what we want to discuss further.

MARK DATYSGELD: Sebastien, would you like to step in just to give us some thoughts?

SEBASTIEN DUCOS: No, I think … I mean, the quote, "and provided that though" wasn't leading to anything else, that it was subject to … Sorry, subject to abuse reports, though, and it finishes like that, it just sounded strange in reading. But I have to admit I didn't go back to the original to see exactly what the full context was.

MARK DATYSGELD: Can we consider that one fixed, Steve, Marika? Yeah? Can we consider that one? And with that, this is our very small list. But since we were rejoined, Justine, would you like to clarify about the statements on the first outline quote? We'll put it on the screen? It's about page seven. We were discussing the different language on this. It would be useful, if you want, if you think that there's anything to add about the statements, this would be a good time to do it.

JUSTINE CHEW: Certainly. Thank you, Mark. Sorry, I had to step out to go to the ALAC room.

Just in relation to the first page, the point I was trying to make was that we had some discussion about whether the buckets that we selected were mutually exclusive. And I think somewhere down in the report, it actually suggested it wasn't. So it's captured within the report itself. It's not reflected in the executive summary. So I just thought that if the small team were agreeable, that we agree in principle that it wasn't going to be mutually exclusive, that you could take a different approach simultaneously, if necessary, to address a particular issue, then I think it warrants a mention in the executive summary. I don't know whether

you need me to address a second point that Greg has just deleted. I think it's similar.

MARK DATYSGELD: Do you want to take that one? Because I think that the first one is … I think we are in agreement and we concur with it. Would you like to follow-up then?

JUSTINE CHEW: Sure. I think the second point that I made was again we had some queries about whether it should be one PDP or a number of PDPs and my suggestion was just to say policy development, full stop, and not enumerate it.

MARK DATYSGELD: That was taken in by the group, so we are 100% with you. Would anybody from ... I think we don't have hands. Marika, are we good? Do we have outstanding issues?

MARIKA KONINGS: I think from the staff side, we would like to do kind of another read-through. We made a couple of changes and things to the executive summary that we want to make sure are also transferred in the other parts of the document. But I think then it's a question for the small team to … If you all want to do a final-final review of this and then factoring in when you would want to submit this to the Council for its review. Just from a timing perspective, the document outline for the October

meeting is the 10th of October with the meeting being on the 20th. So in function of that, you may want to kind of consider a final cut off line. Our assumption at least at this stage, there shouldn't be any "cannot live with" items. We seem to have gone through it all and there seems to general agreement, but of course there may still be minor issues or grammatical or editorial issues that we can of course always, always fix. And of course factoring in the meeting and maybe travel afterwards. Maybe getting agreement on a deadline for final review. From our side, we'll do kind of a clean-up and accepting all these changes that were discussed and make sure they're consistent throughout the document and we can then send a notice to the group when the document is kind of available for final review. But if you can indeed agree on a deadline for that, then we can package it up and you can send it to the Council.

MARK DATYSGELD: From the staff side, does the fifth of October look good? Would that be a reasonable day? Group, does anybody have anything against us setting the deadline for the fifth of October? This would then cover the ICANN meeting itself. Then we get a week to kind of get back or travel or whatever we're doing. Then … Oh, the fifth is Yom Kippur, though. Very well reminded. The sixth, then. On October 6th should be the final deadline where we are done.

It's not the deadline for submitting comments. It's when we're done. Which means that we would have the week between the 29th and the 4th to discuss any outstanding things, and if nothing is heard by the sixth, we are done. Does anybody oppose to that? Perfect.

Final dates for the group is the 6th of October we wrap up or report there and we submit it to the Council to be discussed in the next agenda. So get back to your stakeholders to make a final check. We should be good. I think we're all aligned on this. Definitely no major changes, but if there are small things that you would still like to see tweaked—I said small—we can work on that.

So, with that, as we approach the end of the meeting, I would like to open to any final outstanding questions or comments, favoring the group members first in case they want to make any comments and from the general audience as well, just to note that this would be the sequence. Would anybody like to make final comments?

Sounds good. We just keep it transparent and all members [inaudible]. Paul, any final thoughts?

PAUL MCGRADY: Just a thank you to Philippe for his vision for this small team as Council chair. I think hopefully we have met your expectations.

PHILIPPE FOUQUART: Thanks, Paul. I just want to thank everyone who has been involved in this. I think it's, as you can tell—and as you will tell—with the bilaterials that we will have this week, there's a huge interest in this and everyone is looking forward to the next steps.

So, again, just to reiterate, please reach out to the small team members, your councilors. Next step is not the next physical meeting. It's the next

Council meeting that's next month. So thanks again, everyone. Looking forward to this week. Thank you.

MARK DATYSGELD: With this, everyone, thank you so much for your presence those who are here, those who are online. Your support keeps us going. So, I will adjourn the meeting and feel free to talk to us during the week. Reach out to me and Paul. And if you have any further comments, we are here, we are open and we want to see this being successful. Thank you, everyone. The meeting is adjourned.

DEVAN REED: Thank you all for joining. Once again, this meeting is adjourned. Have a wonderful rest of ICANN75. You may end the recording.

[END OF TRANSCRIPTION]