ICANN74 | Policy Forum – GNSO Council DNS Abuse Small Team Meeting
Thursday, June 16, 2022 – 13:15 to 14:30 AMS

DEVAN REED: Thank you. Hello and welcome to the GNSO Council DNS Abuse Small Team. Please note this meeting is being recorded and is governed by the ICANN expected standards of behavior. During this meeting, questions or comments submitted in chat will be read aloud if put in the proper form as noted in the chat.

Taking part via audio if you are remote, please wait until you are called upon and unmute your Zoom microphone. For those of you in the main room, please raise your hand in Zoom and when called upon unmute your table mic. In the secondary room, please raise your hand in Zoom and go to the standalone mic when called upon.

For the benefit of other participants, please state your name for the record and speak at a reasonable pace. You may access all available features for this session in the Zoom toolbar.

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

MARK DATYSGELD: Welcome, everyone. It's a pleasure to have you all here. This is Mark Datysgeld, co-chair of this beautiful team. Right here we have my good friend Paul McGrady. He has joined me on this mission. Today we would like to repeat some of the things that we have said this week but also advance in other points. So I do apologize if we touch upon things that have been discussed slightly during this week, but ultimately our goal is to move it forward.

So my initial remark is that this group has been outstanding. When we set out to assemble this group, something we had requested for quite a long time, we weren't given a specific remit. It was an exploration project to see what was feasible. Where can we actually get? Within the GNSO Council what are the available solutions, if any?

And many, many, many questions have emerged from our work or outreach with the community. What we will present today is the product of three or four months of very intense work, and this is my initial remark. Thank you to the group for being so committed and for giving us so much of your time and attention.

Paul, I wonder if you have any additional remarks.

PAUL MCGRADY: Thank you all for being here and sorry that I rolled in at the last minute. It was you guys or the cheeseburger, and I picked the cheeseburger. But I didn't turn out to be all that late, I think. Thank you all for all the inputs and exciting ideas that we've already received that we're looking through now. More ideas welcome as this process goes on.

But I really feel that I would be irresponsible to not call out that this group to me has embodied that spirit of multistakeholder collegiality that we all seek and enjoy about this place, and I really would just like to commend everyone for the way in which they've approached this. And I'm excited about the next several weeks. Mark?

MARK DATYSGELD: Thank you. With that, I would like to move on to our progress update. I wonder who is in control of the slides. Is that you, Steve? Yep. Sounds good.

So as you can see here, we started from the idea that what steps can be taken, if any. And this very important because since we didn't have an outcome, it was also very important that we [stick] all potential avenues. And you see as we discuss this matter that very different paths were explored and we had reached different conclusions.

So the main question is what this tackling DNS abuse means. We have been saying this for the past few years. We hear it in different constituencies, in different support groups, support organizations, different advisory committees. But what does tackling DNS abuse actually mean in practical terms? How do we achieve that? And how do we address abuse?

So moving forward to the next slide, if we are looking at this question from the GNSO Council's perspective, there are potential paths that are suited for policy development and there are paths that are possibly suited for other forums, other avenues. And this became quite clear as we are trying to define the problem.

And the team members can probably attest to that. It's not that we stumbled upon the definition [issue] which is something that has been brought up in the community several times over the past few years. But more that we had to define the actual problem, which is different. It's not about what definitions are in the contracts but rather about, how do we actually look at the problem as a community? And this has become foundational to what we are trying to achieve. Next slide, please.

See, when we first started the group the first thing that was decided was we need to reach out to the community because many subgroups were doing progress within the community parallel to each other without direct conversation. At most, they met during [inaudible] in the DNS abuse oriented sessions. But everybody was making progress at different paces, looking at issues from different angles, and not really conversing, not really acting as a body.

So in a sense this group became the forum for that. It became the forum where the different groups were bringing together these ideas, were trying to give some shape to the problem and in time gain a better understanding of what does DNS abuse mean and how can we address it.

So I believe from the feedback that we have heard this week that this goal has been achieved. A lot of community members have approached us and said we feel that our input has been taken seriously, that proper consideration has been given to this issue. And this is in no way [the merit] of the chairs or the staff. The group members are very available to discuss these ideas and advance them.

And certain questions started to come up that perhaps were not available before or were not predicted in this group. So by looking at the data, by looking at the contracts we eventually reached out to ICANN Compliance itself and had a very productive discussion with them. I believe all team members would agree with that. That allowed us to, let's say, reach a better understanding of what does this look like from ICANN's side as well.

So at this point, I would say we have heard from all parties that were interested in talking with this group. The SOs, the ACs, ICANN itself. We had a small conversation with…you know, some of us had a small conversation with the [CEO] as well. I think we understand where we are right now. Next slide, please.

Okay, perfect. As you can see, we received answers from most of the community. And I would say as well that those who are not in this formal list have regardless reached out to us individually. We have heard from the entire community on this matter.

And you will notice that among the parties were involved we have the DNS Abuse Institute. And the reason for its inclusion is something that we as a team discussed how to reach out to different parts of the community. And other organisms were considered. They're very important organisms that could help us with our mission. But given DNSAI's unique role in the community and how it has been working with contracted parties and, let's say, the closeness of it to the process—at least during this particular stage, and this is not final—but during this particular stage we reached out to them as a conveyor of a different perspective so that we would not be exactly locked into our own perspectives and would have this extra.

This does not mean that other groups are excluded from further consultation. It just means that during this first approach we chose to reach out to DNSAI. And this is important to outline because we have heard from other organizations that they would like to have input or in some way dialogue with us, and that's definitely not closed. That's not an avenue that's closed. It's simply that at this moment this is how it was decided. Next slide, please.

And on that point, what did we actually get? Well, we talked about this community outreach. What actually came out of that? I would say all, but let's put most to be academic here, most of the community recognizes the importance of this issue as something that needs to be, as we said on the first slide, addressed. Without exact shape, without a specific direction maybe, but there is no actor in the community who is active, the people in the room, the ones who are here participating remotely, in person, reading the reports be as it may, everybody cares about this issue and thinks we can do a little more.

Therefore as a community we understand this is an issue and we want to advance it. That in itself is good because it lends a lot of credibility to the process and it means that we are moving toward something that's worthwhile for the entire community.

Now to the second point, this was interesting. I don't know if we were expecting one way or another, but the way the answers took shape nobody's really interested in one of those overarching PDPs. This is what we have heard loud and clear from the entire community. Nobody wants to be stuck in these endless discussions that potentially would fragment us further.

And in this sense, a term that Graeme brought to the table that took a little bit of traction I would say, let's call it that, the idea of a micro PDP, a mini PDP, a limited PDP should we say. And, yes, while that's not within the scope of ICANN's current policymaking, the spirit of that idea I believe is one that the team has internalized, let's say.

Go for it.

PAUL MCGRADY: Just before we're reminded that there is no such thing as a micro PDP, we acknowledge that there is no such thing as a micro PDP. And so when you hear that term bandied about I think in this context—that's not to say that the community couldn't develop something called that—but in this context I think what we're talking about is a laser focused PDP that tackles one knowable issue. And maybe instead of me trying to be the secondary force to interpret Graeme, why don't we ask Graeme. What did he mean by micro PDP?

GRAEME BUNTON: Thank you. So when I wrote that letter I was not trying to invent new policy processes nor am I a policy process expert of the GNSO. It was really just trying to emphasize that scoping is crucial and for this work to be effective and timely it needs to be extremely narrow in scope. And so that's really all that meant from my perspective.

MARK DATYSGELD: And beautiful because it's pretty much what everyone in the community was telling us. This can't be the effort to boil the ocean or whatever your regional expression is for this. This cannot be the effort to end all that there is to be discussed and exhaust the subject. This has to be a way for the community to move forward and be effective.

So loud and clear we have heard the community. And the subject of maliciously registered has emerged as a strong point as well. I don't know if it's something that we have become ready to tackle yet. Perhaps this is something that we will be able to tackle in the next few months, but it would be important to acknowledge that we have heard very loudly as well that this distinction between maliciously registered and compromised is important. And perhaps we are not at a point where we can say what does this mean, at least in our personal interpretation and in the interpretation of this multistakeholder group, but it has come up. It is something important, and I think it should figure in future discussions.

And finally, to that final point, it's something that I believe has been heard in different sessions in small tidbits here and there. There are non-policy development activities which are possible. The term here being "possible" because this is not strictly within the remit of the GNSO Council. This is not our, let's say, direct responsibility. But since we did this outreach effort, we have the minds of different members of the community in the small group.

It is something that we can point toward, hint at, or otherwise try to help advance. Not order, not mandate but help. Next slide, please.

And then comes this point. How does DNS abuse relate to the current contracts? This has been interesting. It is something that we perhaps would like to, if any point stands out, I wonder if there's any ICANN staff in the room or in the chat or participating somehow that would like to complement any point that's made. Please feel free to do so.

Because we did have a very, I would say, extensive conversation with ICANN Compliance and asked some pointed questions. The group was given the freedom to ask these pointed questions and truly we can only thank ICANN Compliance for being frank with us, for being open. Because we understand we were asking tough questions.

And at the end of the day, let's put it this way. Within the current interpretation of the contracts and within what is understood to be in the contracts right now, what can be done is being done. Let's put it this way. Which means if there are slight changes to this interpretation or to the contracts, perhaps more could be done.

So if we are unsatisfied as a community at the current outcomes and it is Compliance's understanding that what can be done is being done, then this validates the point of having a group, a small team on DNS abuse within the GNSO Council. Because it implies that there is some kind of change that needs to be achieved for us to be in lockstep for both ICANN Org and the community to be understanding the same thing at the same time. Next slide, please.

So what ICANN Compliance has told us, and this comes as information sharing shall we say, is that things are very dependent on what's going on in that particular contract. Who is the registrar? What is the specific domain? There is no uniform process currently to address these questions. It is more of a per case process.

And in that sense, this is fair because indeed each party has a specific agreement with ICANN and these were performed at different times, so this makes sense. But at the same time it also seems a little difficult. It seems a little cumbersome in the sense that we are trying to address these issues at a faster pace or maybe, let's say, with more power, with a little more strength, a little more bite.

So the question that we posed in specific to Compliance was, if there's a specific domain that is actively harming the Internet within the boundaries of what we currently consider to be DNS abuse, what's in the contract, if that particular contracted party is not responding to you, can you address the issue from your side? The answer is no, they cannot.

Currently they do not have the mandate, power, tools, call it how you want, to address something, a case such as that one. They are dependent on an external party to address that. Be it the contracted party itself. Be it law enforcement, governments. Somewhere down the chain this needs to be addressed.

Which might be desirable, might not. It seems from the feedback that we have received that this is not exactly what we would want. We would want threats of a scale that are actively harming the Internet within the narrow definition that we have right now to be stopped. So this is something to take into consideration.

And if something needs to be changed, the final point, if the definition needs to change or the interpretation needs to change, then we as a community need to bring forward different interpretations, new policy. They will not be able to change it from within the organization. It's not like we can tell them please do this differently. They made it clear to us that if we want something to be done differently, we as a community need to tell them what's the path to do that. Next slide, please.

We have reviewed the entire scope of the outreach effort to us. We have reviewed the considerations from Compliance. We are in the very late stages of engaging in that. And again, if it looks like I'm praising the team a lot, yes, I am. This has been incredible work. Literally, you people have done incredible work. We have managed to go through this in between 73 and 74. This was a very,

very nontrivial effort, and I'm really glad that we got the team that we did because this was no small amount of work.

And now we are setting ourselves an even more aggressive deadline which is kind of finishing going through all of this and trying to understand what can be done between 74 and 75. This is where we are right now. We have reviewed most of what's available. We will wrap this up rather soon, and we will be able to actually understand what are the outcomes that we will offer to the council and to the community.

I wonder, the slides with the buckets, Steve, is it the next one or is it this one? There we go. It's the next one.

And this brings me to, let's say, the innovation of this group, if you may. The small team kind of naturally over the course the process has come up with three what I'm calling buckets. You can call them baskets. You can call them whatever you prefer. The CEO likes fruits. We like appliances. So tables. Whatever you feel is best.

There's the policy development side, and this is GNSO Council material. What should be recommend to the GNSO Council to discuss in the form of policymaking process? What is a PDP? And no matter what we do, I think we're all very set on embracing this idea of small PDP, of narrow PDP.

This can be achieved within PDP 3.0. It's just that it hasn't been explored fully yet, but it can be done. Staff has been incredibly supportive of us. We have been receiving a lot of help from them to understand what is within the scope of the PDP 3.0, and it has been super helpful. So that's bucket one.

Bucket two is community outreach and information sharing. We don't mean to say that ICANN shouldn't be enough to do this, but it also means that we have heard from many parties that they don't understand what DNS abuse is if they are from outside this very small bubble that we are in. This very technical, very informed bubble. Outside of it this is not being communicated properly. So maybe we're doing good inreach but the outreach is not sufficient at the moment.

We have heard from different parties in our normal conversation with other actors from this ecosystem, be them hosts, be them ISPs, be them cybersecurity enforcement people. The message is not coming through clearly enough. How do we work together as a community again to bring this issue to the table?

Because I think something that this group has proven, and ICANN doesn't stress this enough, we are not adversaries. In spite of any other problems the community may be facing in other arenas, we are not adversaries. If you are at the table, if you are at ICANN, you care. The people who do not care are not here. If we are here, we care.

And we should be working together to get this job done because we won’t be harming ourselves. We’ll be harming the people who do not care. The people who are potentially harboring things that we do not care for. So this is bucket number two.

Finally bucket number three, suggestions—I’ll stress the word “suggestions”—for contractual negotiations. It may be that there is a route to get us there sooner rather than later if there is a willingness for contractual amendments to be made. These don’t need to be extensive. They don’t need to be aggressive. Everybody is on pretty much the same page in this. Aggressive changes are for policy development.

Potential contract amendments, simple things, the need to address abuse, period. Something tight, to the point. Something that gets the message across for the actors who are on the table who are sitting here with us. It changes basically nothing to the ones who aren’t and maybe do not care as much. They will have to act.

So this is the kind of thing that we’re envisioning when we say suggestions for contractual negotiations. It’s not earthshattering changes. It’s things that people are already doing in this community and we might need other parties to pay attention to. And with that, next slide.

I don’t want to bore you further. I thank you so much for your attention. I think it was important to get through this entire process together with you so that it is transparent because from inside it has been very transparent. I will hand it over to my good co-chair Paul McGrady to continue the session so that you don't have to keep listening to my voice. Thank you very much.

PAUL MCGRADY: Hi. There's a reminder here from Marika about submitting questions and comments into the chat. Maybe everything Mark said was super duper self-explanatory and everybody is on the same page. If there were questions that came out of that, please do put them into the chat. If there are comments about what we talked about, please put it in the chat. I do see Greg DiBiase's hand up. If you could go ahead, Greg.

GREG DIBIASE: Thanks, Paul. I think that was a really good summary, Mark. I just had some notes as a member of the team, other things that had struck me during this work. When you mentioned the slide on not wanting to get in a big PDP, one of the things I thought was interesting was not wanting to get bogged down in a definition of DNS abuse. Like thinking about malware. Everyone agrees malware is DNS abuse. We don't want to wade into this conversation where we're possibly getting into content which is outside of ICANN's remit.

So I thought that was just kind of an interesting and maybe a little more context about what does getting bogged down mean. Getting bogged down at this stage is expanding the scope of things that are potentially outside ICANN's remit that the community could be butting heads about. So I thought that was interesting.

And then kind of just one note on Compliance. I think you said this well, but I've just been hearing this. I've been hearing Compliance is saying they don't have the tools they need. That's not what they said. They said they have the tools they need for the contract as addressed. And when we said what tools would help you, they said we can't answer that because our job is enforcing the contract. The GNSO, the community sets the policy. They decide what we need or where we could go further. So maybe just a small note, but I think it's worth describing that in context of Compliance's response.

Yeah, and then the last thing, I just put potentially under that contract thing is it's also up for discussion about Compliance's interpretation. That's not the end all. They're saying they don't think they have the power to request mitigation. You could argue that take appropriate response could mean that in certain circumstances they could request mitigation.

So I think that's another thing to consider here is that Compliance's response isn't set in stone. I think take acceptable measures—I should really have this one sentence memorized by now of 3.1(a). Yeah, just adding that as another potential piece. But, yeah, great summary.

MARK DATYSGELD: I stand by everything that Greg has said.

PAUL MCGRADY: Thank you, Greg. And thank you, Mark. I just decided to look up the definition of "bog" because of what bogged down means. It turns out that it may mean something completely different to the British, so I apologize. But it's an area of wet, muddy ground that is too soft to support a heavy body. I think that the community has been bogged down in the last several years trying to get precise definitions. And our reward for that was we got stuck in the mud.

And so it's not that those definitions don't matter. It's not that the issues that would live in an omnibus definition that everybody could agree to aren't important. It's that there are some things that when you see them you know them, as Greg indicated, that they're just DNS abuse. They just are.

And so I think the vision of the last several weeks has been let's get on the things that we know about. And let's start to make some progress. And let's start to get some wins as a community. Let's recognize the wins that are already going on within the community, the independent work that was reported [on] in the process. So I think that is where we are.

Working session. I hope that there is more to that slide than just "working session" because I'm in trouble if not. Marika would like to say something.

MARIKA KONINGS: Thanks, Paul. I actually have a question and a comment from the chat. The first question is from Laxmi Prasad Yadav. It's asking, "What specific points as a registrant we have to consider during contractual agreements with registrar?" I don't know if you want me to go straight to the comment or you first want to see if someone wants to answer the question.

MARK DATYSGELD: I do not consider myself involved enough in this or having enough knowledge. I would like to offer if any of the group's members would have a good answer to that because I particularly at this point don't feel like I have the answer. Does anybody want to offer an answer to that? Greg, please?

GREG DIBIASE: I think from a registrant perspective the contractual agreement in question would be your registration agreement with your registrar. I think it would be important to understand their abuse policies and what may or may not be inside the scope. And I think, I guess going from personal experience, it's good to remember to be responsive. That there may be issues that arise and you need to keep your data accurate and be able to communicate with the registrar to mitigate any potential harms or say this is a false positive. So I guess understanding the registration agreement and making sure you have accurate data so the registrar can reach out if necessary.

PAUL MCGRADY: Thank you, Greg. I see we have a hand up from Seb, and then we have a comment that we need to get to. Seb, go ahead.

SEBASTIEN DUCOS: This is Sebastien Ducos, also a member of that small team and representing the registries. This is not purely related to DNS abuse, registration in general. Just reminding a registrant that registering a domain name is not just a commercial transaction. There are some contractual commitments that are linked to it. Greg mentioned some, indeed, in terms of keeping your data up-to-date and accurate and so on and so forth. Certain TLDs also have restrictions, and when you are asked to recognize them before registering, it's a contract. If that contract is broken, it will have consequences too. So just in general, registrants are part of this machine and have roles and responsibilities too. Thank you.

PAUL MCGRADY: Thank you, Seb. Marika, you have something?

MARIKA KONINGS: Yeah, thanks, Paul. There's another comment from Daniel Prince. I did see Daniel have his hand up earlier, and I think this session is open for anyone who wants to speak. So I'm happy to read his comment but if Daniel wants to speak, that is fine as well.

DANIEL PRINCE: Sure, I'll ask it more or less. I wondered if a micro PDP or a scoping question that might be addressed under this, and I think this would be under your community outreach bucket on the three circles slide, whether there might be an entity, a group, or an individual who has specific expertise with spam or specific expertise with malware or botnet activity that might be able to get their abuse complaint to the top of a registrar's list. And whether we explore whether those…I don't know if that would be within the purview of this. What do you think?

MARK DATYSGELD: I open to all group members to answer. I will give an initial answer and please feel free to follow it up. Yes, when we started this we were considering do we work with the M3AAWG, do we work with APWG, do we work with Spamhaus. That was I think a foundational question. At the end of the day what we arrived at was we do not have the substance yet to ask them for anything at this point, so perhaps we should discuss this again when we know exactly what we would be asking.

And please keep me honest, group members, I think this is where we are at. If we arrive at conclusions that seem interesting in this community outreach bucket, it's looking good, it has good shape, as a community we have all agreed that it's looking good, then that's certainly a potential next step and something to be discussed by the group.

I see hands up, and I would like to give them the voice to speak, please.

PAUL MCGRADY: Seb, is that an old hand or a new one?

SEBASTIEN DUCOS: No, that's my new hand, and I would like to answer if I may, Paul. You point to trusted notifiers. I think that's a very interesting topic. I don't know that it's a topic for the small team itself. It might be for one of those three buckets. There are inherent issues with it and particularly due to jurisdictions and due to other things like that. So I think that there are a number of players in the industry that do work and try to have contracts with trusted notifiers in order to help the work and enrich the data and the knowledge they have of the issue for their own TLDs or their own registrants if they're a registrar. I think it's a lot harder for the community to start imposing those. Suggesting, making this thing, keeping an address book of where to go, but I think it's then so important to let the registries and the registrars given their own legal conflicts to decide who to work with and who they can't work with. Thank you.

PAUL MCGRADY: Thank you, Seb. Before we go on to Thomas, I note a helpful link by Reg in the text. Thomas?

THOMAS RICKERT: Hi, everybody. I think that's an excellent question. And you will all know or most of you will know that I'm representing the ECO Association here, and I think that what we do at ICANN is more or less limited to what ICANN can do due to its limited mandate. But in order really to tackle the topic of DNS abuse otherwise or other types of abuse we need to have relationships with other types of infrastructure providers and other third parties.

And potentially, this group is not the right group in order to do that. And I think it's important for everyone to understand that this is not a reluctance to take care of these issues, but it's just what it is. We are living in this ICANN bubble, but for certain topics in order to be fixed we need to have a discussion with the real world and not with ICANN world only.

Just to illustrate this, when we're talking to abuse departments of hosting companies about DNS abuse they say, what? Because they don't know what DNS abuse even is. They don't use that terminology. And so we need to even change our lingo when we are trying to establish relationships with third parties that are certainly necessary. But we need to make sure that we are meeting them halfway where the understand what we are doing.

And I guess the best way to do that is talk about real life scenarios because that's what they understand regardless of definitions. And then try to form relationships such as the one mentioned in the document that Reg has thankfully pointed to in the chat.

PAUL MCGRADY: Thank you, Thomas. I see Greg's hand.

GREG DIBIASE: Yeah, I think just adding one more point on Sebastien and Thomas' points is that I think from the effectiveness and trust level that's something between the contracted party and that notifier. If nothing else because there are a lot of different business models and ways that these parties operate. So effectiveness and trust, these are kind of amorphous words. But I think if nothing else as a result of the diverse type of businesses we have, I think that has to be between the actual contracted party and the trusted notifier.

PAUL MCGRADY: Thanks, Greg. It seems to me that it would be a very, very difficult thing to legislate trust, right? Trust is built over time. Do we have more questions or comments before we move on?

MARK DATYSGELD: I would like to invite anybody in the room who has comments and who would like to step forward. The group is fundamentally I think all of us are here and we are happy to hear inputs because after this meeting we will delve back into our little world of going through outreach and discussing things. And so if there's any message you would like to convey to us, we would be very happy to hear it at this moment.

PAUL MCGRADY: I think Mark's trying to say we don't get out much.

MARK DATYSGELD: We don't. We spend a disproportionate amount of time on this. So any hands up, this would be a great moment for that. Otherwise, we will probably be moving on with the session. So just give you a moment.

PAUL MCGRADY: Okay.

MARK DATYSGELD: Perfect. So you get to see a little bit of what we do. It's super interesting. You'll be dying to see this. So this is the old version of the document, isn't it? We have a newer one with the questions and all of that. This is the discussion version, the one where we fight over things. Thank you. Can you please magnify that for us, Steve? To any of you who would like to follow the document, it has been posted in the kindly by Marika. So on this first topic—can we frame this slightly better? Thank you.

Malicious versus compromised is a topic that, as I said, has emerged very strongly. But from our discussions as a group it seems that this is a clear concept but slightly amorphous in the sense that the ICANN community hasn't really internalized this concept yet. It hasn't been adopted at scale yet.

Our current discussion is what would be the next step in terms of dealing with this distinction. We have seen it being used in reports. We have seen it being used during our discussions. But how do we actually explore the subject? The answer right now is, I think, I don't know. So I would very much like Marika to….

MARIKA KONINGS: Yeah, thanks, Mark. I just wanted for those that are observing this session to maybe provide a little bit of context about what this document represents. As you explained earlier, we had a lot of input from different ACs and other groups on what the group might be looking at from the perspective of the problem to be solved and what expected outcomes would be. So the group compiled all that input in this document which we've called, I think, the input review tool.

The group already did a first pass through of trying to understand and appreciate the input provided. So for each of the inputs provided, we've already drafted a short summary of what the group considered. Some of the questions it tried to answer to better assess what the next step might be.

And what we did from the staff team's side, we identified some specific questions that seem to be remaining to be able to decide what, if anything, the group wants to recommend in relation to that specific topic to the GNSO Council. So those questions are highlighted in yellow throughout the document. And the hope is that the group can focus on those and try to get as specific as possible in seeing where there is indeed agreement to recommend a certain direction. And I think we've spoken about the three buckets beforehand and seeing is there agreement that that specific suggestion fits in one of those buckets.

Of course, there's obvious interlinkage between some of these comments. As well there may be some further questions or further work that may need to be investigated before that answer is found. So I do think that we'll need to do one more run through. But our hope is by starting here, and then I said we've tried to identify some specific questions that may help the group hone in on that question of what, if anything, you think should be recommended to the GNSO Council on that topic.

So I'm hoping that is helpful context. As we've said before as well, this is staff's approach or questions. Of course, if there are others, if we've missed something, overlooked something, that's really up to the group to add. So I'm hoping that's helpful, especially for those that are maybe new to this conversation.

PAUL MCGRADY: And, Marika, for clarity just so we know what the three things are, they are malicious registrations used for distribution of malware. Am I right? Is that the number one? Or is it a different list?

MARIKA KONINGS: No, I was more referring to the list that the three circles.

PAUL MCGRADY: Oh, that's right.

MARIKA KONINGS: So whether something belongs in the policy. Whether it's something that's more communication outreach aspect. Or whether it's a suggestion for contractual negotiations. For this one, Steve, it may be helpful to very briefly flick to the left side because I think that's what you're referring to, Paul. The three specific topics that were suggested in this comment were indeed these three items.

So I think the question is indeed what we're trying to focus in on. Indeed is this something where the group thinks the time is right to suggest policy development? If so, what is it expected to address. If the time is not right for that, is there anything else that needs to be recommended or considered on these topics? I think that's a bit at least where we were going and hoping that would kind of narrow down what the group would like to discuss.

PAUL MCGRADY: Thank you, Marika. And, Steve, if we can go back to that highlighted yellow now. I've pulled these into the chat, and so we will open this up to members of the team and others in the room or in the overflow room or participating around the world. We'll just see how far we get with the time we have left. Question number one: Is there support to further consider the three topics identified as policy development topics?

Mark, you have something to say?

MARK DATYSGELD: I do. Greg, Tom, John, Justine, Seb, what do you guys think? I personally think that this has popped up, but I'm definitely unsure of how do we advance this because this seems like it may have different implications in different spheres. How do we actually start tackling this? So it would be awesome to see some hands up with your wonderful ideas. No hands up? I'll volunteer someone, I swear.

PAUL MCGRADY: Seb to the rescue. Thank you, Seb. Go ahead.

SEBASTIEN DUCOS: You took my words, Paul. I was going to say it's up to the rest of you, exactly. From my point of view, I don't think that there is much question about bringing that back to the council. I think that we might—and I don't want to get into the weeds of chartering. It's not the purpose at all.

But again, we've discussed that many prolonged hours within the small group what a micro PDP may or may not be and etc. And I don't want to use the term certainly in our answer back to the GNSO because it's going to create confusion. But we might pepper it with hints of what the size of this might be or what the questions might be or something like that. Again, not chartering. Not anything. We're only here to give our recommendations. But

I would add a bit of that just to contextualize and clearly explain what we see the size of these things being. Thank you.

PAUL MCGRADY: Thanks, Seb. Marika, your hand is up.

MARIKA KONINGS: Yeah, thanks, Paul. Actually, a question I have myself. And I see Graeme is in the room here. Because I think I heard him mentioning yesterday—and he's trying to hide. No hiding here. But I think I heard him mention during one of the sessions yesterday that the DNS Abuse Institute is actually working on a paper that would break down what the difference is between malicious and compromised domains and what kind of actions could or should be taken.

So just wondering if that is something that's relevant for this conversation. Would that help the determination on whether policy development would be a path or is that more a best practices recommendations outreach kind of suggestion? So I just wanted to flag that.

GRAEME BUNTON: Thanks, Marika. If I can jump in on that briefly. That work is actually coming out of the contracted parties house DNS abuse group. And so the registries and registrars are collaborating on this discussion paper about that distinction as well as a few invited people from the security community.

And so it's not really a best practice but it does go into the various options about how to mitigate harms that are malicious, which mercifully is generally simple, and how to mitigate harms where it's a compromised website where it becomes more complicated.

That work is a little bit stuck at the moment, but that's almost entirely because I've been busy with other things that I have harassed you with all week. That work, we're really aiming to have out at or just ahead of the ICANN75 in Kuala Lumpur. We hope it's useful for developing the community understanding of those issues is really the goal of that paper.

MARK DATYSGELD: Thank you for adding that, Graeme. A follow-up to that. It has been brought up, and I think this is still a bit of a point of contention, what do we do with the compromised website? I think that this has become kind of a sticking point in that situation. I think we all agree that maliciously registered, great. That's perfectly the scope of what we are here to do. It is our technical responsibility to get rid of that.

In terms of compromised websites, there are two ways of looking at this. On the one hand, it is potentially not the owner's responsibility. It has been compromised. But on the other hand, it may be presenting an active threat to the Internet. So balancing out those factors and creating correct escalation paths, finding the right balance seems to be a bit of a challenge and something that we will have to look into. And it's kind of at the core of, I think, what we're trying to discuss.

I see hands up.

PAUL MCGRADY: So we're going to go to…Marika, is that an old hand? Okay, we're going to go to Greg here in a second. But specifically the three ideas deal with malicious registrations, not compromised domain names. And so I want to make that clear.

And then we're going to hear from Greg here in a second but, in the meantime, I want to give everybody a thought project since we're coming up on time. Which is, are these three ideas better ideas together or better ideas one at a time? Because when I look at this I think some of these are more straightforward than other of these. So off to Greg.

GREG DIBIASE: I unmuted my computer instead of my mic. In terms of initial steps, I think there's also a step here. In a lot of comments there was conversation back and forth on the merits and potential cons of a PDP generally. I think we've done a pretty good job of identifying what we'd want to address. But there is still…I think we'd need to lay out for the council potentially some concerns that are raised for a PDP, some advantages of the PDP and maybe walk through that. Because I kind of feel like we're on the same page regarding subject, but that seems like a preliminary step before we dive into questions on do we do one or all or what would be the scope here.

PAUL MCGRADY: Thanks, Greg. Any additional reactions to these three issues? Mark?

MARK DATYSGELD: I will react then. I wonder if our staff support would help us clarify one thing. When we make this distinction maliciously registered versus compromised, do we know already if this is covered anywhere within the scope of current policy work? Or is this something new that has been brought to the table that we do not have a direct way to recognize yet? Because that's potentially important. If we're going to target maliciously registered, it's very important that we understand that we have the provisions to actually achieve that. That we have the understanding of what that is.

And I see, okay, we have quite a few.

PAUL MCGRADY: All right, Greg, I think that's an old hand. Next up is Graeme and then we have Justine and then we have Susan. And I expect that will take us to time. Graeme?

GRAEME BUNTON: Thanks. There are a couple things in there I'll try and address coherently. The malicious versus compromised distinction I think is relatively new to this community. We've really only been talking about it, let's say, in the last six months, a year or so. Compromised very clearly gets into working with registrants and hosting companies and I think often outside of ICANN's remit. And so that's why very deliberately when I was writing that letter to this team, I didn't even address it.

And I think malicious registrations where you have some sense that the intent of that domain name is to cause harm keeps this within ICANN's remit and is far easier to address. And so I think getting into that work is very complicated, and I would encourage people as they're thinking through these to really try and tackle the malicious issues first. And I think that gets us now back into the ordering in one or sequential.

I just think the community needs to try something in a very, very hilariously narrow scope to see if you can get output, to see if you can make some progress on these issues. Do that, and do that a few times, before you start getting into the weeds on stuff that involves other communities and people outside of ICANN's remit, etc. Thanks.

PAUL MCGRADY: Thanks, Graeme. And important to that which is by not getting into compromised domain names nobody is conceding anything, that it's in scope, out of scope, whatever. But by separating it out essentially what we're doing is we're punting on those, saving it for another day. Going in on something I think that, as Graeme says, it's very attractive to think about a hilariously narrow PDP where the community gets a win and Grandma is in less danger than she was three months ago, right? And I think that there's something about how progress and success begets progress and success. And so nobody has to feel like they're losing out on a discussion about those two kinds. It's just that what we're talking about now is something that is narrow and designed to move things ahead.

By the way, I said we're running out of time but I was reminded that we have 15 minutes more than I thought we did. So for those of you that thought you were getting out of here, I apologize. We're up to Justine. Go ahead, Justine.

JUSTINE CHEW: Yes?

PAUL MCGRADY: Now we can.

JUSTINE CHEW: Thank you. Sorry. Yeah, my reaction to this is…well, it takes a few facets, I suppose. Number one, I am a bit concerned that we are—and no offense to Graeme—but I'm a bit concerned that we're getting bogged down by this use of PDP. I'm not ultimately convinced yet that we necessarily need to go the way of a PDP because the question that comes up in my mind is, even if you look at just maliciously registered domains, how do you identify which domains are maliciously registered?

And following on to that, of course possibly these kinds of abuse if it can be established clearly then possibly requires a heavy-handed approach in which maybe something can go into the contract. In which case you need a PDP to do that. But we also know that we don't actually need to go the PDP way to get some things into contracts.

And juxtaposed to that is the compromised domains because I guess that requires a little bit of a nuanced approach. So a lighter touch, per se. So I can see the reasons for differentiating between maliciously registered domains and compromised domains. Thanks.

PAUL MCGRADY: Thanks, Justine. An important here, right? There are two ways to get things in a contract. One is a PDP and the other is through contract negotiations between ICANN Org and contracted parties. And if there's a groundswell on some of these subjects, nobody will be sad if it happens sooner rather than later, right? But that's not what council can do, and so we're kind of only talking to a certain extent what council can do. And then what council can't do, it may have to cheerlead for the rest which is perfectly fine.

UNIDENTIFIED MALE: [And that's a suggestion.]

PAUL MCGRADY: Yeah, that's the suggestions bucket. Right. Okay, so we have Susan Payne up next. Susan, please go ahead.

SUSAN PAYNE: Yes, thanks very much, Paul. I'm responding to the question I think you were asking. And so first of all I'm going to repeat it back in case I've misunderstood what you were asking.

But my understanding is you've got these three different groups of malicious registrations that you're talking about. So the ones you put in the chat. So the one is malicious registrations used for malware, those used for phishing, and then the ones used for operation of botnet and command and control. And I think you were questioning what this group thinks about it. Should they be dealt with separately or all together. So I hope that was the question.

And in response to that, without at all wanting to derail anything or change the direction that perhaps this group was thinking of going in, I just had a question of is there any data one way or the other in terms of whether there's overlap amongst these groups?

I'm thinking in particular of one and two. Is there data that suggests that many domains used for malware are also used for phishing or data alternatively that suggests that really the area of overlap is miniscule. Because that may very well make a difference to whether it makes sense to deal with them together or separately.

MARK DATYSGELD: Thank you for the input, Susan. We do not have the hard data. Let's put it very, very clearly that the hard data is not in because even from ICANN's perspective they're not giving us that hard data. It's something that we have to guestimate based on our talks with the contracted parties and from the external cybersecurity providers that we rely on. So the objective answer is, no, we do not have definitive data.

The other answer is based on what we have seen or what I have personally seen or been relayed. Usually, websites are tailormade for a purpose. You would not usually operate a botnet and use it to phish and something along those lines. Normal procedure is that a botnet will serve its purpose. It will generate an algorithmic domain and it will bounce between them and serve that purpose of communication. Generally very fast.

Its own category of abuse actually because it's so much more sophisticated than the others. The others require people to actually enter a website. So for people to be infected by malware or to be a victim of phishing or be the subject of pharming they have to enter the website. For botnets they just generate domains, register them massively, contact each other in fast succession. They can drop in, drop out. It's a subject of its own, let's call it.

So if we were to bundle—again, my personal perspective—botnet is one thing, the rest is something else. Botnets are kind of an active threat while the other threats are likely more passive. That is my personal understanding of the matter. Hoping that this addresses at least the spiritual question. And going back to the queue.

PAUL MCGRADY: Thank you, Mark. And I think the other distinction—and actually I kind of divide them up differently. It's interesting. I think of the distinction between them is that one and three seem to be more of a kind because either they are or they're not. Where phishing there is sort of that looking at how brands and copyrights are used in that process. And so that one to me seems to be of a different flavor. It's interesting Mark and I are co-chairs and have different views on that. But all good inputs.

So we have Steve. Steve, you're next. All right.

STEVE CHAN: Thanks, Paul. Really just a procedural point. When you're looking at I guess this type of topic, so the maliciously registered domains, it can be considered from a couple perspectives. So you can look at it from the three buckets. So there's maybe different ways to approach it that you all talked about earlier whether or not it's policy development or other mechanisms. So that's one thing.

But the other part that I wanted to mention is you can see it in the way that this question is drafted. The approach that the small team could take, it could be different things. So if the group is not convinced that policy development right now is the right move, it could actually do interim steps. So it suggests in the text here that maybe scoping is necessary. And that could help gather some of the data that you all might need to make an informed decision.

Which may also inform, to Susan's question, maybe some of these types are overlapping. Maybe they're discrete. So even if this group might be leaning toward policy development on this set of topics, there are still interim steps that could take place to help provide more data and, like I said, make a better informed decision. Thanks. That's all.

Actually, one small thing. There is a—I'm on RP duty too now—there's actually a comment too if you don't mind.

PAUL MCGRADY: Yes.

STEVE CHAN: Sure. So there's a comment from Chris Lewis-Evans. He says, "When it comes to dealing with compromised domains, I/Public Safety Working Group would love to support the understanding of [how] we deal with victims and how this might help inform the actions taken when dealing with compromised domains." Thanks.

PAUL MCGRADY: Thank you, Steve. And Mark asked Chris to contact him or me or both of us directly later. We'd love to have a follow-up conversation on that. Next in the queue is Greg. Greg, please go ahead.

GREG DIBIASE: Yeah, I think that's a really good question by Susan. I think it kind of goes back to my initial thought that the first step here is outlining the potential pros and cons of the PDP that were identified by the group. I think this is just another question noting on the subject of one or three groups, we note that it may be more efficient to deal with them separately. But we also note, and let's try to find the data where we can, there may be overlap between these different types of abuse and basically we [have to] flesh out all the potential issues. But that's the first step is basically looking deeper at questions like the one Susan raised.

PAUL MCGRADY: Excellent. Thanks, Greg. And that makes sense, right? The stuff in yellow may be a bit premature. We need to take a step back and do that and do some thinking around it. So that's a good outcome from today. And, Susan, thank you for that. And also Greg. And we have John McElwaine, the gentleman from the south.

JOHN MCELWAINE: Wow. All right, thanks, Paul. So I'm not on this small team, so forgive me if I'm stating something that you already talked about and decided against. But I'm wondering if a possible course is instead of doing a micro sort of test run of DNS abuse is actually to look at it from a macro perspective.

And I don't know if you've gone through this exercise, but let's presume that somebody has made an allegation that fits a definition of DNS abuse. What would be the steps that we would expect would be undertaken by a contracted party, and what impact would that have or need to have on the contracts that they have so that we could then analyze whether there would need to be any policy development?

And bring it all back to what seems like the current plan is, that could be going on. You could take a very micro slice and also look at those issues. So you may have had this discussion. But that's what I'm most curious about is whether there has been any broad level discussion as to what the process would be if DNS abuse, if we could come to an agreement as to what it was and whether something was compromised or not, what would be the process in dealing with that? So I'll see if you have any comments on that.

PAUL MCGRADY: Yeah, John, thank you for that. To a certain extent that is both something that we need to do in the world of imagination but we also need to leave enough room for a PDP to do the specifics of that if the PDP is the way to go, right?

And I'm going to say something that I don't think is controversial in this room. What we're really talking about is what we need the bad guys to do. We heard in a session yesterday about all the stuff the good guys are up to.

And so to a certain extent while we do that imagining we need to be thankful and aware of the good work that people in the community are doing and maybe going to them and asking them, "Okay, we're imagining what the outcomes of the PDP might be. Remind us again in some level of detail what's the ordinary step that an ordinary good guy registrar or an ordinary good guy registry does?"

And in doing that it may take some controversy out of it if we're basically just asking the good guys to do what they're doing and asking ICANN to help the bad guys start doing it. Yeah, Mark?

MARK DATYSGELD: Thank you. So very briefly to that point, I think that one thing that we heard from the community in our outreach effort was that, and I agree fully, the CPH and its extended community has been acting in a lot of different fronts on this matter. In just this meeting we are seeing two tools built that will help us tackle abuse. And I know for a fact there are more in the pipeline.

So there is this groundswell of innovation in fighting DNS abuse that we need to be mindful of in the sense that we do not want to create a process that will somehow not work together with that. And the innovation is happening very fast. It's an accomplishment of the contracted parties house, and we definitely do not whatever goes to the GNSO Council to be adversarial to that.

We want it to complement it perfectly and work within those boundaries and create the right synergy that whatever work the CPH is doing by itself continues to flow as best as possible and we're actually augmenting that. We're working together with that. How do we achieve that perfect balance? I think that's in the challenges column.

But it's the reason why we're not trying to look at this so macro is because literally the pace in which this is progressing is pretty fast and we like that. As a group we like to see that people are making huge progress on this. So how do we not stop this progress and rather help it? That's, I think, something we will spend the next three months trying to balance out. What's the role that we have in that sense?

PAUL MCGRADY: Terrific. We are at time but Justine's hand went up just under the clock. So we will let her have the final word on this, and then we'll turn this back to staff to tell us what's next.

JUSTINE CHEW: Thanks, Paul. I was just going to react to what you said a little while ago about good guys and bad guys and also what Rubens put in the chat. I think from the perspective, the way I see it, we would do well if we understood what the good guys, contracted parties, both the registries and the registrars, are doing in terms of identifying maliciously registered domains and tackling those abuses from that kind of registrations. See if there is as standardized process that would be amenable to being adopted somehow, maybe through the contracts.

And again, it's not really to penalize the registries and the registrars that are doing well in tackling issues. It is more about having something, and preferably in the contracts again, that ICANN can use to knock on the doors of the bad guys. The contracted parties that are not doing things that they should be doing so that they can be called out or given notice that they are breaching a contract and therefore consequences can be taken through that way. Thank you.

PAUL MCGRADY: Thank you, Justine. And just a quick note to say I loved being together. I love being together in this session. I loved being together all week. I feel like we got more done in four days' time than maybe we have in the last four months. And I think that this face-to-face notion is a really terrific part of the ICANN culture. So thank you all for being here. Mark, last words before we hand it back?

MARK DATYSGELD: Yeah. It's a tradition of the group to leave a hot moment at the end for any group member to vocalize anything that has come up, any impressions. It's just the way we run this group. So I would like to open that moment for any final brief considerations the group members might have. If there are none, I'll hand it back to staff. So looking for any hands. Perfect. This is how we keep our transparency. Let's keep going that way.

PAUL MCGRADY: Marika, Steve, take us away.

MARIKA KONINGS: Yeah, thanks. So the homework still stands, of course, on this document. I think it would be really helpful if small team members can go through the questions and maybe already provide some initial input or their responses to these questions. Because that will help facilitate the conversation instead of waiting for the next meeting. And I think on that point the question is next meeting. Our people are ready to already meet next week, or do you all want your traditional week off after an ICANN meeting? I see some nodding for the week off, so I think we'll just go ahead and schedule that meeting for a little bit less than two weeks from now in the usual timeslot.

PAUL MCGRADY: Go away.

MARK DATYSGELD: Thank you, everyone. It's a pleasure to be joined by the community. Those who are online, those who are in person. We remain very available. Please talk to the co-chairs, talk to your representative within the GNSO. We want to continue hearing from you. Have a very pleasant afternoon, and see you soon.

[END OF TRANSCRIPTION]