MICHELLE DESMYTER

Hello and welcome to the At-Large Plenary - Progressing the DNS Abuse Mitigation Agenda. My name is Michelle DeSmyter, and I am the Remote Participation Manager for today's session. Please note that this session is being recorded and governed by the ICANN Expected Standards of Behavior and ICANN Community Anti-Harassment Policy.

During this session, questions or comments will only be read aloud if submitted within the Q&A pod. Interpretation for today's session will include English, French, and Spanish. If you would like to speak, please raise your hand in Zoom. When called upon, virtual participants will be given permission to unmute in Zoom. On-site participants will use a physical microphone to speak.

Please state your name for the record, the language you will speak, if speaking a language other than English, and please speak at a reasonable pace. And with this, I will now hand the floor over to Justine Chew.

JUSTINE CHEW

Thank you, Michelle. Welcome, everyone, here in the room as well as online. I'm hoping that we can get as many participants as possible because we have some audience participation at the end. First of all, my name is Justine Chew. I'm going to be the moderator for today, and I would like to, on behalf of the ALAC, thank all the panelists who are here, both in the room and also online.

I will say and I would note that we've had apologies from some of the panelists that were invited, which is why in some of the slides you'll see later on, we won't have anyone speaking to us from the Registry Stakeholder Group, the Registrar Stakeholder Group, and GAC. Unfortunately, they had to cancel last minute, but it's fine. We can still carry on. We're just having a conversation anyway, so we're not deciding on anything. With that, can we have a look at the agenda, please, Michelle?

Okay, so, in the short time that we have, we're going to try and tackle three things, which is the first part of the agenda would be just to gain a reflection from our panelists, some of them are participants or members of the Policy Development Process One. Sandra, can you mute, please. Yeah. On Associated Domain Checks.

So, we've had a series of four sessions for that PDP, and I would just like to invite some of the panelists to just share whether they see any issues, whether they think that it's going well and so forth. And then we will spend a bit more time on the second topic, which is to do with domain generation algorithms. And for that, we are privileged to have someone present from the Public Safety Working Group of GAC to just talk to us about an existing framework.

And we'll have a discussion after that to see how we can move that forward. We'll also get some comments from John, as well as

Mukesh. Mukesh, it was supposed to be Teresa, so he's impersonating Teresa today. And last of all, we're going to be talking about what other gaps should we line up in terms of the DNS abuse mitigation gaps. We know that the community has provided some input to the GNSO Council process in identifying priorities in terms of which DNS abuse gaps to address first. And we have already a series of three.

So, the first one is going to be tackled by PDP 1, or is already being tackled by PDP 1. The second one is going to be handled by PDP 2, which will come further down the line. The third one is the second topic here that we're talking about, domain generation algorithms. And for that one, there is some indication on whether that should be handled by a PDP or maybe an outside PDP community process.

So, I'd be interested to get a perspective from the panelists as well as community members here, whether that should really go through a PDP process or does it need to go through a PDP process. And in terms of the audience participation, we have a poll just to seek a temperature of the room as to what you think should be addressed by this DNS abuse agenda.

So, what should be the fourth gap that we should tackle, fifth gap and so forth. Yeah, so, let's get going then. So, can we get to the next slide, please? I think we have an order of speaking. Okay, I've done this. Next slide. Next slide, please. Okay. So, we're going to go into the first part of the agenda today. And the questions are really about what are your thoughts on what's happening with the PDP 1?

I'm going to start with the panelists, obviously, give them privilege. And if any of the audience here would like to chime in, then please put your hand up in Zoom or find a way to indicate. And we can get to you if we don't run out of time. I'm on a tight schedule here. Okay.

So, we have a particular order by which I'm going to call on panelists. If you're not ready, just indicate you're not ready, and we can put you at the back of the queue. So, we have from the CSG, the Commercial Stakeholder Group, our panelist is Ching Chiao. So, can I hand the floor to Ching, please?

CHING CHIAO

Thank you very much, Justine. Ching Chiao here, representing the ICANN BC and also the CSG this time. Thanks for having me. As Justine described, I'm one of the members, but I can only speak on behalf of BC and CSG. I noticed that some of the other members of this working group are also in the room. So, yeah, feel free, as Justine pointed out, feel free to chime in.

But yeah, to answer this particular question, the general sense that we have at least from BC point of view, we have really had a great start for this working group. It's a very constructive start. Many thoughtful engagements across the stakeholder groups share recognition that the abuse mitigation remains the priority of this community.

Having said that, point number two that I'd like to try to make here is that we acknowledge the fatigue in this community talking and working on tackling the DNS abuse policies, but also like to acknowledge that the fatigue is also outside of the community. The attacks on the organization and their customers, and also many of the cyber security professionals that I work with through my job, the fatigue is there in terms of damaging the continual causes of tackling DNS abuses.

So, let's recognize that. Some of the thoughts, if I really need to bring on under that first two statements, is that the BC and the CSG still have concerns about the timeline. The challenge that we're dealing with on one hand is the PDP process that's probably it's now being laid out by the staff that this potential PDP could end at the end of 2027.

And in reality, is that we don't know that the threat landscape or the DNS abuse landscape would change to 2027. And then speaking of maybe it would take another year or two to have the CPH to implement those policy change. So, we're looking at the timeline of 2029 to get this particular PDP to get implemented.

So, knowing that the DNS abuse campaigns often unfold in days or not hours, the timeline remains a concern to us. We also like to point out, I've also pointed this out already in the working group mailing list, is that knowing or detecting or observing the ADC is one thing, and actually to do something, to clean things up or to medicate is another. Right now, this two-part, detection versus medication, it has a great gap there.

We'd like to lay out these facts in this particular ecosystem, that it takes time as of now, as we're speaking fighting the ADC, and then cleaning up the bad faith, the actors who's utilizing those ADC and conduct DNS abuse incidents, those has a huge gap there. I would like to point out another issue about something that will probably won't change, but I like to lay it out for your better understanding that for this particular PDP, the scope of the PDP is very narrow.

So, we're talking about only one registrar and all the ADC under that one registrar. We're not talking about multiple ADC under multiple registrars. But let's do one thing at a time. Let's solve that particular one question first. Probably just allow me to conclude my statement by saying that for CSG, our participation, I'd like to just say that the CSG's advancements of the ideas on combating DNS abuse is definitely brought in good faith.

We're seeking to cooperate. We fully understand that ICANN is the stewardship of the DNS. Even all the wars in the past few years and many years ahead of us, the DNS abuse is not going away. In fact, it's going to intensify in the next few years in the best of our senses. But we're here, the CSG is here to work together with you all to solve the problems. So, we look forward to working with the group and we look forward to working with everyone here in the room. Let me stop here. Thank you, Justine. Thank you all.

JUSTINE CHEW

Thank you, Ching, for that input. I hope you're paying attention and we can have a Q&A or a discussion or other reflections after the panelists have had to go. So, I apologize. I should have said that the panelists should stick to maybe three to five minutes so that we can make up time. Michaela, welcome. You are next on our queue.

MICHAELA SHAPIRO

Thank you so much, Justine. And thank you, Ching, for kicking us off. I really appreciate the opportunity to be here. Michaela Shapiro, for the record, representing the Non-Commercial Stakeholder Group. So, Ching has already brought up a few of the topics that I was excited to bring up today, one of which being, perhaps to scene set a bit, we have really just started the work.

So while we're feeling very optimistic, just wanted to level set a bit to say that we really have only had one discussion already on the substance of the charter. So, we kicked off a discussion yesterday on the first charter question about what should trigger an associated domain check. And so, nothing has been set in stone quite yet.

Even the timeline is still being discussed, but from the initial discussions, the Non-Commercial Stakeholder Group is keen to ensure that this timeline, that we don't do this overly rushed. While, of course, to Ching's point about DNS abuse is an evolving landscape and there are very real security and safety concerns that we want to ensure are addressed, we also want to make sure we do this right.

We don't want to rush this. And the solutions must be balanced and consider the interests of a broad range of stakeholders, including end users and registrants. So, this is also why the Non-Commercial Stakeholder Group is particularly excited to see human rights impact assessments being integrated throughout the policymaking process.

This will be a really exciting new area of work that we can integrate from the start of the Policy Development Process. We're also, just Ching said here as well, we're not trying to address all types of abuse here. We really want to develop a process and a framework that can be applied across abuse types.

So, the idea being this can be future proof and this can be a process that can be utilized, ideally, for a number of, as the threat landscape evolves, it can still be addressed in that sense. Just to add a couple of small things, we're also particularly excited about the scope of the PDP itself and want to remind folks that we have a narrow charter for a reason, and so, we want to make sure that we stick to that particular charter and the framing of it.

And that was deliberately said and agreed upon by the Council. And we again just want to emphasize that a reasonable timeline is very key here, so again, we don't want to rush this, let's make sure we do this right. I'm sure there's more that I'm missing and I'm sure folks have more to add here. So, perhaps I'll pause there and happy to answer any questions and come in again at a later stage. Thank you.

JUSTINE CHEW Thank you, Michaela. Yes, you pointed out correctly, and it's also echoed by Michele in the chat. We are talking about DNS abuse as defined by ICANN. SO, we're talking about five things, really. We're not talking about general internet abuse. A lot of it is probably something that we can't deal with directly in ICANN. So, I'm going to move on to the GAC, the Government Advisory Committee Public Safety Working Group. I don't know if Janos, Noam, and Wolfgang want to speak separately or just have one person speak.

JANOS DRIENYOVSZKI Good morning, Justine. I would speak on behalf of the GAC PSWG. Can you hear me well?

JUSTINE CHEW Indeed, please.

JANOS DREINYOVSZKI Perfect, thank you. Yeah, as Michaela mentioned as well, that we also, of course, we're very in the early phases of the PDP 1 and the effect. In the other four sessions, there was one that really dealt with the substance of the PDP. We also, of course, the GAC PSWG shares the optimistic sort of approach. We are also very optimistic about it and very actively contribute to hopefully speedy outcome of this PDP 1, which is meant to be quite targeted.

And for that reason, we are also hoping that a timeline would be the right one that we settle on in the end and we manage to deliver within a time frame that reflects accurately this targeted nature of this PDP which meant to be a narrowly scoped PDP which addresses a very specific issue of associated domain checks.

Therefore, we're really hoping that this PDP will be, in fact, one of the first examples of delivering something efficiently under ICANN basically, in the ICANN framework. I also take note of what Ching said about addressing the gap between detection and mitigation. I think it was a good point he made that indeed we also believe that the actions taken under this new policy, potentially new policies, evolves the whole action that is triggered after actionable evidence is available for the contracted parties.

And so, aspects like the time to react, the reporting of the results of their actions, and of course the accountability, the enforcement by compliance is done in a way that will result in an efficient policy that can be monitored also. So, it's a policy that addresses DNS abuse, and then also gives some feedback on how this type of abuse is mitigated in the end. And we have a good sense of its workings and operations. And of course, there's sufficient enforcement of it.

So, it's a meaningful tool, basically. It's a meaningful policy to avoid this sort of whack-a-mole approach to DNS abuse, which of course is the current state of affairs that we're trying to change here to have a more coordinated approach that helps both the community that I represent, the law enforcement community, but also helps the contracted parties themselves of saving time and effort to fight the DNS abuse and domains that have been abused. I will stop there. Thank you.

JUSTINE CHEW

Thank you very much for that, Janos. Yes, let's move on to my colleagues, Steinar or Kathleen. Which one you is taking the mic?

STEINAR GRØTTERØD

Yeah. Hi, this is Steinar from At-Large. First of all, I do agree, it was a very good start, and it's very interesting to hear the different approaches from the different stakeholders into this. From At-Large perspective, we haven't written anything in stone yet. I'm not sure we're going to write anything in stone.

But to my understanding, and talking to different particular registrars, I think one of the importance that we will try to achieve here is to make some sort of a policy, a consensus policy, that, frankly speaking, force the bad registrars to do something. Because the majority of the registrars is already doing something, this policy is also that the ICANN Compliance have the tool to police and do something with those that are, it's not a good word, but bad in a sense.

Also, very interesting that we are getting more into a proactive approach for discussing DNS abuse, mitigation DNS abuse. So, I definitely look forward to the outcome of this. Hopefully, it will be as quick as indicated. Some rumors say this can be done in a month. I'm not sure about that, but let's be optimistic. So, Kathleen, you want to chime in on something? No? Okay, back to you then, Justine.

JUSTINE CHEW

Okay, thank you, Steinar. I'm going to allow a little bit of time if anyone wants to make a comment, but not too many, I guess. We do have something in the chat that some of our online participants are asking about, I think mostly related to the human rights impact. So, I wonder if any of our panelists would like to address that point, if there are no other hands. I do see Volker's hand up, but let's put it this way.

If any of the panelists would like to address the question of the human rights impact in the chat, please put your hand up and I'll call upon you. But in the meantime, Volker, please go ahead.

VOLKER GREIMANN

Yes, thank you. Volker Greimann with Team Internet, I'm with the RSG, but here in a personal capacity. I note the efforts that have been going on in the comments that have been made. I feel that having come back from a lot of thought on the topic, we are thinking too small. It's not bad registrars, it's a bad ecosystem in a way that even members of the BC could be doing more to fight abuse.

There are players that should belong in the BC or that are within their remit that made billions by aggregating the ads and directing victims to sites put up by bad actors that are profiting off the abuse. There are players in the ecosystem of the internet that are not contracted parties that are profiting immensely from this kind of action, and they're not being addressed.

They lean left to go on their merry ways. Bad actors that are being shut down by contracted parties pop up at another contracted party. They're just switching the venues where they're going, changing their methodologies from time to time when they have been at various marketplaces because the information-sharing mechanisms do not exist.

If I take down a bad actor on my registrar, he will pop up at Luke, then he will pop up at Michele, then he will pop up with other registrars, and there's currently no real mechanism or process to address this. I think we're thinking too small. We need to address this from a large ecosystem perspective, and this goes beyond contracted parties. This affects everyone. Law enforcement must be involved much deeper.

They must arrest those bad people. I didn't want to use the expletive here. Because only after they are taken out of circulation will they be stopped from putting up those sites again. We, as contracted parties, have a very limited resource. We can take action within our own little walled gardens, within our own small ecosystem, but they are not thinking about that. They are acting across the industry.

They are acting across registrars. When I say that we operate multiple registrars, I see that certain campaigns come in through one registrar with one reseller and another registrar, which is retail only, they open up accounts. So, when I see the same actor coming through various channels on our platforms, then I know for a fact that they are also active on other registrar's platforms, and there's no real way to stop that from happening.

So, even if I take action immediately, they will just switch registrars, activate other domain names that they have been using. And we need to address this from a bigger perspective. And everything that we were discussing right now is just more. That's not saying that we shouldn't be doing anything. I'm just saying we need to start looking bigger when we move ahead on this topic. Thank you.

JUSTINE CHEW

Thanks for that insight, Volker. I don't think anyone in the community would be opposed to that. It's just a question of how do we get there, that's always the case. I didn't see anyone kind of trying to address the question about human rights impact. I will just mention, before I hand the mic to Michele. Oh, have you put your hand down?

But just before we get there, I do want to say, and I'm speaking now in my capacity as the ALAC liaison to the GNSO, in terms of the human rights impact assessment, there is assessment that's built into the PDP process or PDP 1. And I think what I understand is it's getting built from the front end, built into the process of the front end rather than the back end, which is what has happened in the past recent PDPs.

So, I think it's going to feature a lot stronger in the deliberations of the PDP. And that also includes things like global public interest, data protection, and one more which slips my mind at the moment. But suffice to say that the PDP is structured in a way to take into broad considerations of other things rather than just the DNS abuse aspect of it. Michele, do you mind if I just give you one minute, because I need to move on?

MICHELE NEYLON

No problem, but the idea of you giving me one minute I find comical. Sorry, it's Michele for the record. So, as I think Volker covered quite a bit of territory, which I won't go back into. On the human rights aspect of this, people need to be very, very conscious that there is a risk of knee-jerk reactions with any kind of policy that's implemented, that it's very, very easy for smaller registrars, those that are not aware of the bigger context, when they see something coming through as a policy, that they will over comply.

We saw this happen with the most recent DNS abuse modifications to the contracts where domain names were being pulled down by some registries based on a single report from a single random anonymous user on a random social media platform, which is a bit ridiculous because then it takes two or three days for us to find out, first off, who to contact in the registry to get to, who can actually take action to get the domain back up, and then to actually convince the registry to put the domain back online.

And during all that time, all services associated with the domain name are dead in the water. That is hugely problematic. Because the thing with these policies, while you might look at them as being a way to clean up the internet, there are people out there who will use this as a way to target their competitors.

They will actually weaponize the policies to target competitors, to target competing businesses. And there are nefarious actors out there who know how to use these policies against us, which is grateful. Thanks.

JUSTINE CHEW

Thank you, Michele. Yeah, that's duly noted. I think that's a position that the registrar's constantly reminders of. I'd like to move on to the second topic. If I may so next slide, please, Michelle. Next slide, please. Okay. So, here, as I said earlier, we have the privilege to have a better understanding of the existing framework on tackling domain generating algorithms that causes abuse.

As far as I know, the domain generating algorithms are a technique of malware that creates many, many, in some cases hundreds or even thousands of domain names that the bad actors then use to do bad things with, if I may just put that very simply. But I'm going to invite Janos to talk a little bit more about this and as I said, what has been done and to see then how we can take it forward as a community. So, Janos, over to you, please.

JANOS DRIENYOVSZKI

Thank you very much Justine. So, it was my colleague and good friend Gabe Andrews, who is my other co-chair of the Public Safety Working Group, who was behind this initiative but I'll try to present it to the best of my abilities. So, basically, what this framework is about is basically to address, or my presentation rather is about why these domain generating algorithms are tough to handle as law enforcement, but also as registries.

And why is it important to get the law enforcement registries and ICANN on the same page about how to coordinate responsible action. Next slide, please. So, basically, this framework is a voluntary framework. So, it's not a binding framework. It has been drafted by the Government Advisory Committee Public Safety Working Group and the Registry Stakeholder Group.

So, it's a voluntary non-binding framework and it doesn't affect consensus policy. That said, as also Justine mentioned, domain name generating algorithms are often used by criminals to prevent their online activity being detected. There are computer programs that automatically generate domain names, usually using a long random collection of numbers and letters.

This is done at scale and pace to allow the criminals to move between different domain names to continue their activities. For example, to distribute malware. So, the intention of these bad actors is to evade security countermeasures that are designed to prevent criminals from reaching victims, such as blocking the domain on a network. These types of attacks tend to be large scale and well organized with significant consequences for victims.

So, as you see it on the slide, there's a list of, on the left side you see what is the main characteristics of DGAs. And on the right side, you see the impact of those characteristics. So, these are very inefficient to block DGA-generated domains, as thousands can be generated. It's very easy for criminals to re-register another domain from this pool of generated domains, just to retain control, again, over a botnet to distribute malware.

And even after seizure, these DGAs keep generating valid future domains. And so, the impact of that is that for law enforcement, because of this ongoing sort of generation, they might need to return to the courts to renew their seizure. Authorities, registries need to process thousands of new domains, orders, and they can also incur significant costs when creating these and sort of the cycle, then repeats. Next slide, please.

So, why is it important to get this cooperation a bit more efficient between law enforcement and registries? This framework, the DGA framework, addresses the role of both of these stakeholders in specifically handling malware and botnet infrastructure using the domain system specifically as a result of course illegitimately used DGAs.

Now, the DGAs are often although employed by botnet command and control infrastructure to maintain the control over the botnets, this framework might not be limited only to DGA referrals, it may also be used in handling non-algorithmic large list of domains employed by botnets or malware. But basically, the two main tools to address this from the registry side is to reserve the domain or to create a domain.

So, reserving a domain is when registry places the DGA domains on its reserve list. Therefore, any attempt by criminals to register that domain that has been put on the list, the create comment will be rejected. So, why is it efficient? It's because it prevents criminal registration of those DGA domains that have been generated that was meant to be used for DNS abuse. It doesn't require any permission from ICANN based on the policies and the contracts.

The registries can act immediately, and therefore, it has a low administrative overhead. But on the other hand, it has some limitations as it does not enable sinkhole the domains which are useful for identifying infected machines and also to notify the victims. So, this measure is the best for time-sensitive blocking where sinkhole is not required.

So, just to explain basically a bit, sink-hauling is when a registry redirects the name servers of the domain which allows for law enforcement to help identify victims of the malware or those who have machines participating in a botnet. So, this allows more time to gather this information. And the other measure is to create the domain, so the registry itself, register the DJ domains, then log suspends or redirects, i.e. sinkholes the domain.

So, botnet traffic then is captured and it can be analyzed. What it solves, as compared to reserving the domain, it enables sinkholing, so helps identify machines and victims. It also supports active victim notification, remediation, and also provides intelligence for ongoing law enforcement investigation. The requirement, of course, for this is it has some contract restrictions under the sections put in the brackets there.

So, registries must obtain permission and also fees apply. But the framework also addresses this through the ERSR process, which is an acronym for the Expedited Registry Security Request, which is sort of a fee waiver provided by the contractual obligations so that the registries can rely on this waiver when creating a domain that is on the DGA list. Next slide, please.

So, the objective of the framework is to develop a common understanding of the problems facing law enforcement and registry operators in combating, of course, malware and botnets, as I mentioned, associated with DGAs at a large scale. So, the framework really aims to address also the scale issue of this problem. It intends to explain how the main is going to support malware and botnets through these DGAs and also the unique mitigation practices that I mentioned in a previous slide.

So as you see, these are the four main pillars, how this framework guides both the law enforcement to provide accurate and timely information for the registries so they have enough time to act to get the waivers if they need it for the creation of a domain and to find a long-term solution basically that prevents from law enforcement from renewing for example their court orders on an annual basis, and it creates a sustainable reaction when it comes to addressing DGAs.

And of course, I really invite you to read the full paper that has been released by these two stakeholder groups. It's only 10 pages. And in the end, it has an annex also that provides a template on how to apply, HOW to fill out the request for the ESRS P-waiver. And so, I find it a very clear and sort of useful document. And of course, hopefully this framework provides inspiration also for other areas of the DNS abuse where this could be replicated.

So, you should really see through that lens is that this was based on practical examples. There were two cases also, real-life examples, where we're taking them as a basis, and through those examples, solutions were found to create this voluntary non-binding framework that allows both parties, both the law enforcement and the registries, to act in a coordinated concerted manner which saves time, saves effort, saves cost basically to sustainably address this kind of abuse that is committed by domain generated algorithms.

I'm mindful of the time, so I'm going to stop there, but of course, if you will have questions, I will try to answer them Thank you.

JUSTINE CHEW

Yes, this is Justine. So, thank you for trying to keep the time, Janos. I see a hand in the room, the Zoom room. Volker, I'm just going to ask you whether it's a question or you're going to make a comment. Okay, I'll allow a question. So, please go ahead, Volker.

VOLKER GREIMANN

Yes, thank you. The question arises from a lack of understanding because we see DGAs as tools, just like guns or scripts or algorithms. There are tools to generate lists of domain names that can be used for any purpose. Many are being used for bad things, so what differentiation are we making between DGAs being used for good, for bad, or for neutral purposes? Or are we looking to throw out the kids with the bathwater and ban the use of DGAs altogether just because some are being used for bad? Thank you.

JUSTINE CHEW

Wolfgang or Naoum, would you like to take that?

NAOUM MENGOUDIS

I can take that. Thank you. Naoum from Hellenic Police. Of course, when we locate a DGA algorithm, we have first to verify that it is used for abusive purposes, for example, phishing campaigns or system dissemination. And if it's verified, and if it's reverse engineered, we know what they see this and how the domains are being randomly generated, then we can mitigate it using this framework for swiftness.

JUSTINE CHEW

Okay, thank you. Can we go back to the agenda just very quickly, please? Yep, next slide, please. Okay. We're gonna get into discussion right now, but before I open the floor to both panelists as well as folks in the room and in the Zoom room, I'd like to invite, I suppose, John first, and then Mukesh.

Okay. I'd like to invite John first to just kind of address what's being talked about in the room as well as, I think, one of the key questions that we have for you is what role should or could ICANN Org play in this area especially in terms of better coordination? Could ICANN play the role of the overarching coordinator? So, over to you John.

JOHN CRANE

So, I'm going to add one thing to that, and that is what has ICANN traditionally done in this area because obviously we’ve got like 15 years of experience working with people outside and inside the community on tackling DGAs. So, what we could/should do really depends on what the policy looks like and what the contracts look like. And I don't mean to be flippant about that, but I don't think we necessarily want ICANN staff going off and designing their own things, so we have policies for that.

Now, I heard the comment about information sharing, and that's what you've talked about. We recommended in a painful discussion in 2010, the concept of actually having a centralized information sharing solution way back when that came from staff, and it just wasn't prime. And I'm seeing a lot of these conversations about whether or not we need better information sharing, et cetera.

And with a little bit of humor and a little bit of nostalgia and I'm actually glad to see that these discussions are coming back about how we do this. And even back in 2010 when we put the proposal, it wasn't necessarily that ICANN should do this work but there was a need for this kind of coordination. So, that's an interesting discussion. That discussion came partially because of what ICANN was doing in the late 2000 into 2010 around DGAs.

There were some particularly malicious malware out there that were starting to use this technology. The most famous one of them is probably Configure. So, we've been working over the last decade or so, much less so now, because I think the methodology is understood. But in those early days, we spent a lot of time working with law enforcement, public safety groups, and scientists to try and determine what this methodology was.

Once you've actually reversed engineered a DGA, it's not enough just to get a list. And my law enforcement colleagues here will know this, a lot of work is done to ensure that you're not victimizing other people by taking down the DGAs. There's a lot of methodology that goes into actually looking into all the names, deciding whether or not a name should be created or blocked or reserved with the terminology using the new framework.

So, we've been working quite extensively over the last 15 years with law enforcement and people in the operational security community, precisely so they understand how a domain name system works, what it means to register a name versus to block a name, many discussions about what you do as far as sinkholing, how is that going to work? We had lots of discussions about pushing things to park pages versus pushing off to DNS servers, et cetera.

So, one thing ICANN can always do is be a subject matter expert around how the industry works and try and work with the people that are trying to combat abuse so that they can work effectively and get the results that I think we all want, which is a better public safety. So, we don't really get into those kinds of discussions anymore because I think people actually understand the methodology.

As this evolves, we are happy to continue giving that input. If the community comes up with solutions that require policy, we will implement that policy. So, if there is a PDP around this, whatever comes out, we will implement it. Now, if what comes out of these

PDPs is extensive, because don't think that setting up some kind of coordination effort that passes data around is something easy.

We're not the only industry trying to tackle this issue about how intelligent sharing, data sharing happens, and how you do that securely and how you do that in the right manner. So, something like that, if it went down that road, would be probably a multi-year project. For example, it's not in our strategic plan or our operating plan at the moment, which means it's not budgeted and all those kinds of things that you need to do as an organization. But we're definitely here to follow and to play our role.

We've made adaptions in the past. We've heard a comment about the ERSR, the response. We've had many of those over the years, and I don't think we've ever said no to one. That's my colleague Mukesh to talk a little bit about how we've evolved that over time, because these things don't stand still. I think the ERSR was from 2009, but Mukesh, maybe you could talk to a bit about where it is today.

MUKESH CHULANI

Thanks, John. So, the ERSR was a service specifically catering to registry operators, and we saw a presentation on the four point framework that had that as the last piece. But we noted, and this is in part to what John mentioned, the evolution of existing processes might also take place. Because the industry is moving and we received notice that registries were not the only ones who required the ERSR because registrars were also being named in court orders for example to take action.

And so, the ERSR at that point would have waived ICANN's fees for registries but did not waive fees for registrars. So, we created, not that we created, but there was resulting unequal treatment. And so, we rectified that in 2021. So, the ERSR is actually an outdated term. We should no longer refer to it. It's now called the security response waiver because it's not just for registries.

And the security response waiver covers three things. Malicious activity involving the DNS of such scale and severity that it threatens systematic security, stability, and resiliency. An occurrence with the potential to cause temporary or long-term threat impacting the registration of domain names and a court order from a law enforcement agency with jurisdiction which requires the entity registry or registrar to take action. So, those are the those are the ground rules, and this is evolution as we saw it was needed.

JUSTINE CHEW

Okay, thank you, Mukesh. So, what I would like to see, and I'm going to allow a little bit of time for discussion, but before that, if I can ask Wolfgang, Naoum, or Janos to just address the question in chat from my colleague Steinar, that would be much appreciated. Just reply in the Zoom chat.

What I would like to see in the time remaining that we have for this topic is that we have heard a high-level overview about the framework itself, and we noted that some of the terms are now outdated, and we know that it has been in existence for a while.

So, the question really, and I would like to try to prioritize the panelists, is how do we take all this information and figure out what to do with it to move this forward? Because as I said, one of the questions is, do we need a policy development process for this? Is it something that's better tackled outside of policy development process by cooperation with the community?

In which case, which part of the community needs to be at the table? All of us? How do we make that happen? So, if the panelists could try and address any of those questions, if you want to put your hand up and I'll call upon you. I did notice that Ching had his hand up earlier, so I asked him to wait till this part to make his point. So, Ching, do you want to take the mic?

CHING CHIAO

Thank you, Justine. Ching Chiao, once again, from the BC CSG. So, actually, yes, to respond to Justine's question. So, I guess the initial reaction that I have after hearing John's very great talk and took us back many years of work, I believe that one missing piece as of now in this room also getting the ccTLD on board because the DGA took place as many of us in the industry saw that it's not just happened to the Gs, but also the CCs.

So, that's number one. And maybe an observation or a question that I have is that for law enforcement colleagues in this room, or for the GAC colleagues in this room, I've noticed in some of the tactic, if I may, is that the sinkholing, the techniques of getting a cease-and-desist site page may not be the most effective way as of now.

Some of the more sophisticated law enforcement agencies that I witnessed from the sidelines is that they intentionally leave some of the malicious names. So, they intentionally keep those malicious names and still let them up and running and let those malicious and the botnets, IPs, or the domain names, the network of IPs and domain names to call homes.

So, they need those to be mapped out, and then pretty much to wait patiently and then to map out all the DGA clusters. So, I'd just like to leave it as it is. Thank you.

JUSTINE CHEW Thanks, Ching. And I believe that John would like to respond to that.

JOHN CRANE Just partially, because from my own knowledge, going all the way back to the 2000 ccTLDs, this is very much a voluntary process by registries and registrars. There's not policy about how you do this. There is now policy that you need to mitigate DGAs, but there's no policy about saying how you do that.

And of course, although CCs are not covered by that policy, most of the ccTLDs I've ever worked with do actually participate. So, it's not that they're not because I know for a fact that many of them do. And I'll leave the other stuff over to our PSWG colleagues, I think, because it was a question for them.

NAOUM MENGOUDIS

Yes, thank you. Naoum from Hellenic Police. Regarding the question of the chat, if I understand it correctly, maybe it can be rephrased, the registry reserve some domain so they cannot be created before they will be created because knowing the generation algorithm, we know what point in time some domains will be used, and it's put on a reserve list and then they can be, of course, unreserved.

So, they can be framed after that. I don't know if that was the exact question. And regarding some police forces workflows that they can keep running some DGAs or some botnets. Usually, by sinkholing, we want to protect the victims and track the infected machines. So, we can contact them for notification or we can have some statistics.

Sometimes, some police forces, when they take over a server, we have first to take over a malicious server, like the command-and-control server, then we can keep it running, like not running and infecting other machines, but pretend it is being run so we can learn more about the network or locate the offenders. Like it's not just left running and infecting people.

JOHN CRANE

If I may, the outreach to solve the infection base is actually also, I wouldn't use the word sophisticated, but it is broader than the impression you gave because there are organizations, for example, there's an organization called Shadow Server, who I know work a lot with many law enforcement that collect a lot of this data and then have mechanisms for internet service providers to find out about their infection base and for national certs, et cetera.

So, we tend to think about this from our perspective as like registries and registrars, and it's about the blocking and the stopping of the DGA. But what I found over the years that a lot of the important work is actually about getting to the infection base and actually solving some of the harm to the end users.

JUSTINE CHEW

Okay. Thank you for this very enlightening conversation. Can I just ask you to put your hand up in the Zoom, please because I'm monitoring that. We do have a couple of minutes more for this topic, I don't really want to stifle the conversation here. So, I'm happy to try and incorporate more.

I'm going to recognize Michele, and Steinar, if you want to put your hand up, please do that. Otherwise, I will just make another call. If anybody wants to make any comments, please put their hand up in

Zoom so it's easier for people like me to follow what's going on, who wants to say something. Michele, please go ahead.

MICHELE NEYLON

Yeah, thanks, Michele here. This thing around the DGAs, as John rightly points out, there has been quite a lot of cooperation between ccTLDs. The ccTLDs have a lot of flexibility in how they do this. They're not restrained by ICANN contracts.

So, ccTLD, like for speaking as a registrar for .ie domain names, when we saw an uptick of certain types of abuse which meant quite a large volume of domains was registered, we were able to go to the registry and go, hey, these were all registered for nefarious purposes, whatever that was, whether it was DGAs or not, it's actually irrelevant, because they were able to go, yeah, no problem, we recognize that.

Here, we were, A, killing the domains, and B, we are refunding it. You are not being penalized financially for doing the right thing. And that, I think, is the key point here that some people seem to be missing. The fact that either a registry or a registrar would be financially penalized for trying to take bad crap off the internet is the dumbest, most ridiculous situation in this entire circus.

It makes absolutely no sense to me, and I don't understand how anybody with a straight face can defend it. On the registrar side, we have very, very strict limits on the number of domain names that we can delete in what's called the add grace period. But basically, when a domain is registered, first five days, we can delete the domain. However, due to a variety of things that I'll go into now, the limit on that is actually quite low.

Now, for a large registrar, so take, for example, I'll pick on Volker. So, Volker's registrars, they have quite a large volume of registrations per month. So, as it's a percentage based on that, the number of domains they can delete without being penalized is also quite high.

As a much smaller registrar, if we are targeted by scumbags, which happens from time to time, that means that the number of our deletes goes up dramatically, and we go past the threshold. The policy at the moment is so restrictive that it would cost me literally thousands of Euro in administrative overhead and registration fees to potentially get a refund.

And if I do it once in this quarter, I probably won't be able to do it again for another three or four quarters. So, that to me is farcical and is something that might need to be addressed. And I would see it as being more of a problem than this entire associated domain check thing, which operationally is going to be absolutely impossible to implement. Thanks.

JUSTINE CHEW

Thank you, Michele. Yeah, I guess I agree with you as well, which is why we want to bring forth other things that we can do possibly outside of a PDP and things that we may think as priority. Okay.

Steinar. I'm sorry, Siva, I have to cut the queue off because we need to move on, but I'm going to allow Steinar since I recognized him earlier. So, Steiner, I'll give you one minute.

STEINAR GRØTTERØD

Yes, this is Steinar for the record. And just for clarifying what I was asking in the chat here is, is it really possible to create a list for the registry that it prevents it from being registered? And is that list something that you have to monitor on a daily basis to add, remove, adjust, et cetera? It's just to understand this problem from that point of view. Thank you.

JUSTINE CHEW

Naoum, you wanted to say something?

NAOUM MENGOUDIS

Yes, thank you, Naoum. Yes, of course, since you have first to reverse engineer the DGA, the algorithm, and when you have reverse engineered it and you have the seed phrase, you then know at what point in time what domain will be generated. So, you know today, it's like Tuesday, 10:30, we know that the domain, the algorithm will generate a specific URL, domain name.

So, if you know it beforehand, you can block it. Maybe you may put it in a long list and like our registries can access this list and check if a domain that is being is going to be allocated is in the reserved list or you can run your algorithm yourself every time by checking like would this be a bad domain included in the DGA or not and you can block it like dynamically.

And regarding Justine's question about if this could be solved by best practices or by policy, I think of course best practices is the first step and coordination, but maybe policy will be needed afterwards for everybody to comply.

JUSTINE CHEW

Okay, I think that's the first that I've heard, that possible suggestions of taking this issue forward. So, thank you for that, Naoum. Siva, I have to move on, so I would invite you to put your comments or question in the Zoom chat, please. Okay. So, thank you for that discussion.

Michelle, can we move to the next slide, please? Michelle, next slide, please. So, I'm sorry about this technical hiccup. Michelle or whoever's controlling the slides, can you please move to the next slide, please, so that we can move on? Okay, great. Thank you. Thank you.

Okay, so this is the section where we try to encourage things that should be on the radar of GNSO if they want to tackle it as a PDP, or if they don't, then indicate possibly maybe find another way to do it. Like for example, if it's a best practices format, maybe we can get community involved and tackle it outside of a PDP. Next slide, please.

So, I'm just going to ask the panelists to talk about maybe one or two of their priorities, and that is outside of the three that have already been identified, which is associated domain name checks, the API, batch registration issue, which is PDP 2, as well as tackling domain generating algorithms, which we just talked about.

So, I'm sure that there are other things buzzing in their bonnets. This is your time to have your say about what should come next as item number four or gap number four, five, six, whatever. So, the order that I have now is, again, prioritizing the panelists, the invited panelists. So, I don't know who wants to take this from the Public Safety Working Group.

JANOS DRIENYOVSZKI I can take it, and then of course Naoum can come in, of course, to compliment.

JUSTINE CHEW Okay. Go ahead then.

JANOS DRIENYOVSZKI Thanks, and this Janos for the record. Within the GAC and the Public Safety Working Group, we would be interested in exploring further accuracy of registration data. That is still, we believe, not in the place where it should be when it comes to the whole supply chain of not just registrars, but then you have the resellers, the privacy proxy providers and so on.

So this is still an issue that needs to be believed that should benefit from policy. And in that regard, I can refer to the GNSO Preliminary Issue Report from 2025 September that identified gaps in this area regarding timely contact verification or regarding no post-registration identity checks for suspicious activities.

So, we see some gaps that were identified in that GNSO issue report that could be perhaps developed further. Another one would be, for example, the transparency of reporting itself, which we believe it could use a bit more clarity of what data is being exactly held by contracted parties and what's being reported to ICANN compliance. These are just two areas.

The third one is a bit, as you mentioned, Justine, is connected to the associated domains and DGAs. It's, of course, it's a broader category of proactive actions and approach and measures, which overlaps a bit with what we are already doing. But yeah, those would be my initial thoughts and the thoughts of the PSWG.

JUSTINE CHEW

Okay, I'm just going to pause there to say that whoever's in the room and in the Zoom room, if you could pay attention to what the panelists are saying, because there's audience participation after this, and you get to rank certain things. So, if what they are proposing, what the panelists are proposing, is not in that poll that's coming up next, then please also tell us. Just very quickly, please, because we are running short.

NAOUM MENGOUDIS

Yes, thank you. Naoum again. Personally, I would go for the subdomain abuse because I see it a lot, especially in phishing campaigns and malware campaigns. Subdomains are abused a lot because they can spoof the real domain, like my mobile browser's address bar will just show the first part of the domain.

And, for example, if this is PayPal login, something, I may get fooled to do it. Of course, there are other reasons that they abuse subdomains, but I think it's an important gap to consider. In general, apart from all the listed gaps, I think that as Volker said, we should try to make everything work across the whole ecosystem.

Like for associated domain checks, it's not enough for each registrar just to do its own. There should be some information exchange or some signals exchange to be done across the whole ecosystems, between registrars and registries, et cetera.

JUSTINE CHEW

Thank you for that. Can we move on to Michaela, please?

MICHAELA SHAPIRO

Thank you, Justine. Michaela Shapiro for the record, representing the Non-Commercial Stakeholder Group. So, here, a couple of priorities on our end really focused on the process in which we're addressing DNS abuse mitigation. And so, when we think about this, a priority for us is ensuring that there are accessible standardized recourse mechanisms for registrants and those affected by abuse-related actions.

So, this looks like there are a number of ways that this could take, but it could be perhaps establishing pathways for registrants who perhaps have demonstrated that the abuse has been addressed or that the action was taken mistakenly, that they have a pathway to request for that domain to be restored.

Separately, we're also thinking about complaints and appeals processes, so a clear and fair process through which registrants can file complaints or appeal mitigation actions. And this is applicable across types of domains, or sorry, across different types of domain abuse. Andone of my fellow co-panelists, Janos, mentioned transparency reporting.

That's something we're also particularly interested in, that we might be thinking about this framing slightly differently. So, for us, it's really about how the domain abuse related actions are taken. So, what is the decision-making process having clear transparency around what kinds of mitigation actions are taken.

And as I mentioned, the kind of the process in which those decisions that we come to these mitigation actions. So, happy to answer more questions about that, but I think that's it from my end. Thank you so much again.

JUSTINE CHEW Thank you for being so concise, Michaela. Yeah, Michaela. Ching, we have you next.

CHING CHIAO Thank you, Justine. Ching Chiao again from the BC CSG. I'd like to echo what the PSWG, the emphasis on the subdomains is also the very core concern of ours. Speaking on the personal capacity, I'd also like to emphasize on the potential, the DGA or the BAC domains, on what I've repeatedly emphasized in the previous couple of days, on the slow burn of a cluster of a DGA or a cluster of the ADC, which could take many, many days.

And then not to mention the subdomain, which potentially could build on top of those ADCs or DGA names can run into different campaigns. But once again, going back to the question, subdomain is definitely the focus after bulk and DGA. Thank you.

JUSTINE CHEW Thank you, Ching, for also being concise. Steinar or Kathleen, who's taking this?

KATHLEEN SCOGGIN I'll take this.

JUSTINE CHEW Okay, Kathleen.

KATHLEEN SCOGGIN

Kathleen from the ALAC. So, I think that we're going to get a lot of information out of this PDP on whether the model of identifying a very narrowly scoped issue and then having information not only about the gap itself, but also a potential redress mechanism to deal with the gap before we even start the PDP is effective or whether we're just kind of expanding the hole that we're playing whack-a-mole with.

And if we decide that post-PDP, whatever that means, if that was not an effective model, if we move towards more proactive measures like predictive algorithms, et cetera, and that from the ALAC perspective, if that's of more interest and better serving the end user.

And that will obviously have a different scope and take a different level of effort from all of us in this room and also a range of actors. I think we'll see after this PDP, but that is a direction of travel that I could see happening, and that would be of interest to the ALAC. Thanks.

JUSTINE CHEW

Thank you, Kathleen. So, now we get to the audience participation section, which is actually the other here. And thankfully we have enough time for that. So, can I pass the task of getting input from folks here and folks in Zoom to Kathleen, my colleague. Kathleen.

KATHLEEN SCOGGIN

Sure. If we could go to the next slide. So, for some audience participation today, we've taken a few of the gaps identified in the GNSO report. This is obviously not expansive and does not cover even everything that we've talked about in the session today, but we've laid out five different options here.

So, what we talked about, about DGAs, and then registrar contact verification, real-time detection, predictive algorithms, and abuse fees and threat data. It's laid out a little bit on the slide what each of those are. We're going to put up a poll shortly. Just to kind of get a temperature of the room on what we should prioritize next.

And if you think all of these are totally wrong, there's also another option and a second question that will come up in the pool of if you're answering other, what should we be prioritizing? So, just trying to get a little bit of information out of folks here.

So, I'm going to keep the slide up for just a second so people can read a little bit, and then we'll put the Mentimeter pool on. So, if you have a phone to use, take that out, and we'll scan the QR code in just a sec.

JUSTINE CHEW

Sure. What we can do is we can go to the next slide first so that people can scan the QR code and then we can come back to this slide. I think staff is also going to put the link to the Mentimeter in the Zoom chat. So, if you want to use your computer or instead of your phone to get onto the Mentimeter, then you can do that as well. So, hopefully someone's putting that link in the chat.

All right. Okay, so I have been informed that it is in the chat. So, we are just going to let people have a few seconds to decide which way you want to go to get to the Mentimeter, and then we will go back to the previous slide where the questions are. Okay. So, shall we go back to the...

Okay, let's go back to the previous slide so that people understand what we were asking in the Mentimeter poll. So, we only have limited time or limited space to explain what we're trying to do here. I would add that these are the five that were picked out of the GNSO issue report, the final report, that have been identified by GNSO as being gaps that if you address it, then it's a preventive measure, because At-Large has a focus on doing things that are preventive rather than curative.

We know that curative will always be there, but we need to pay a little bit more attention to preventive measures. So, this is based on what's in the report. Again, as Kathleen said, it's not exhaustive. If you see something that you think should be prioritized and it's preventative in nature, then please do also tell us.

KATHLEEN SCOGGIN And I think just for staff, once we complete the first question, you'll have to click as the administrator to initiate the second question, which is where people will be able to write in those additional options. So, we'll give it a minute, but then we're going to want to advance to that second question.

MICHELE NEYLON

So, it's Michele. Since you're all doing stuff with the metric, I think I'd ask a couple of queries, make a couple of comments. Looking at some of the options that you put forward there, it's not very clear to me when this would take place or when you expect to use this. Because there's like three, four, and five in many respects are duplicative and definitely overlap.

But also as well, some of them are not things that are really within the scope of what a registrar or registry could really do. Like, we literally have no ability to do some of these things potentially. And then also as well, I just do wonder about things like, I mean, I see the word algorithm and that gives me a cold chill.

JUSTINE CHEW

Thank you for that input, Michele. So, as I said, we drew this out of the issue report that's done by GNSO. We welcome your feedback if you want to put something in the other. So, it's just collecting the temperature of the room, so to speak. But it's based on some consultative process that has happened so we're not starting from scratch. It is what it is in the issue report.

Yes, and you're right, some of these are duplicative. So, we've taken the trouble to say, for example, like in option two, to combine two gaps. So, potentially we could consolidate a few more. And these are the sort of input that we would like to be able to go back to council on. Yes.

MICHELE NEYLON

Yeah. Thanks, Michele, again. Look, I don't want to get into too much into the weeds. But I think it would be like looking at two or three people coming up with a list of potential issues or things that they'd like to explore might be a nice academic exercise. But when it comes to the actual reality, when you talk to registrars and registries who are dealing with abuse mitigation at scale, things like, for example, register and contact verification, it's very easy to focus on that.

But we see that the scumbags are really, really, really good at faking ideas or stealing entire identities. We had an issue, just as one example, in the last six to nine months, where we got a phone call from a lovely lady from somewhere in Asia who was very, very curious to know why on earth this random company in Ireland had been taking money out of her bank account.

We were very curious to know how on earth we were taking money out from her bank account, because we didn't know who she was either. And it turns out that somebody had managed to completely take over the poor lady's online banking and was generating throwaway virtual credit cards within her system and getting past all the two-factor authentication and all the other security devices that everybody considers to be the silver bullets of the internet world these days.

But the red-stand contact verification, not at all helpful. Predictive algorithms, things like that, the question, again, is you have to understand how domains are sold. So, like, Volker is wholesale, he doesn't have the contact details or see the credit cards of anybody who's actually buying a domain name. He has his customer.

I'm actually his customer in many instances, and that's the same for a lot of the channel. We don't have access to a lot of this data. And again, algorithms scare the hell out of us. And I think Michaela can probably speak to why she finds algorithms a scary, scary, scary concept.

JUSTINE CHEW Yes, thank you again. So, again, this is drawn from a list that has been… it's a product of a consultative process that we've done with the community. And the points that you're raising, I'm pretty sure are being raised by your stakeholder group in Council. How are we doing on the results? I'm just mindful of time. We have seven minutes left. Kathleen, do you want to?

KATHLEEN SCOGGIN Yeah, I think we should show the current results. It'll continue to update for us to have later. But if we could show the current results of the poll, that will also allow us to go to the next question where you can write in your own options. So, if staff could put that up on the screen, that would be very helpful.

MICHELLE DESMYTER One moment, Kathleen.

KATHLEEN SCOGGIN Thanks.

JUSTINE CHEW And while that happens, I see Michaela's hand. So, Michaela?

MICHAELA SHAPIRO Thank you, Justine. No, Michele was right, I did have a couple of concerns about AI generated or use of algorithms for AI abuse mitigation, but that can be an aside. And I'm sure my counselors for the NCSG are doing an amazing job representing this. Sorry, Michaela, for the record. Just a small point here. I think there's an important distinction to be made here with this question as well.

On one hand, there's a question of what are preventative-themed DNS abuse mitigation issues more broadly, and there's the question of whether this should be addressed by way of a PDP.

I just wanted to kind of draw out that distinction here just to say that these may be very valid concerns, but I would encourage us to consider whether a PDP and addressing this via ICANN is necessarily the answer for all of these. I don't have a clear answer on that, but just wanted to put that out there. Thank you.

JUSTINE CHEW Yeah, thank you for that comment, Michaela. Yeah, so the question is actually what should we be addressing by way of PDP next. So, it's basically a way of us just finding out from people who are participating in this Mentimeter poll to understand what they think is a priority. That's not to say that it will be a priority. It's still up to GNSO Council to decide what happens next. But it's feedback that's going to go somewhere.

KATHLEEN SCOGGIN And if staff could also just advance to the write-in option, that would be very helpful. Thank you. Hopefully it triggers on your mentee. Let me know.

JUSTINE CHEW I hate a quiet room. So, while that's happening, I would invite anyone, if they have any comments, to just use the time that we have to chime in. I don't see any hands in the Zoom room. I appreciate that some of this information might be quite hard to digest. So, insofar as you are able to provide an informed input, please do. Again, this is not something that's going to be set in stone, it's just a temperature of the room thing. Michele.

MICHELE NEYLON

Justine, I know that you don't like silence and neither do I. So, I think that we finally found some common ground. Awesome. I think some things that people might need to think about is other ways of mitigating abuse. There are technical things that can be done and should be done and might need to be done. You can look at things like DNS resolver technology.

There are several of the public DNS resolvers and some of the private ones that offer layers of security within them so that they check against various lists, they block certain types of domains, they can block entire TLDs, they can do lots of different things.

Now, some of it, of course, does raise issues around human rights and speech, and I'm not going to ignore that, but there are solutions out there. Like, for example, if you have an internet connection in a school, you probably are limiting access to, I don't know, Pornhub, for example. I can't imagine that it would look particularly good if primary school students were able to access hardcore porn instead of learning their alphabet.

And that's probably a place where it might be appropriate to mitigate some of these issues. Because a lot of the time as a registrar, we only have very, very limited ability to do things and we can only do things in certain places. Not everywhere. I cannot remove an image from a website that's using a domain that's registered through us unless it is sitting on our servers. It's physically impossible for me to do it.

If you were running some kind of reverse proxy or something like that, you might be able to do something with that, but we can't. And the other thing as well is that, that coming to ICANN always as the solution to all forms of internet abuse, I think is a little bit disingenuous, because it's kind of this thing of saying, hey, we came to them, we asked them to fix something, and they refused.

Whereas in reality, a lot of the issues are outside that. Volker talked earlier about some of them. Like certain domain names, the only way that anybody ever gets to them is from an ad. They're not typing them into a browser, they're not finding them as a link from another website, they're not being shared within friend groups or anything like that, they're only being pushed to us in adverts on various platforms that we all use. So, maybe those platforms need to clean up their act a little bit.

JUSTINE CHEW

Yes, thank you for that. Yeah, it's hard to fathom the whole universe of DNS abuse, let alone internet abuse. So, I guess all of us are trying to find ways to play a part in mitigation. I'm also mindful of time and I don't want to keep you from lunch. And I didn't see any kind of input on the second question. So, can we go to the last slide, please? I'd just like to conclude.

Thank you so much for the panelists who have been able to join us, either in person or by remote participation. Much appreciated. I hope you will consider accepting our invitation again should we have something on in Seville, which I think could be likely, and may not just be an At-Large and ALAC session.

To all the participants who are here in the room and also in the Zoom room, thank you very much for your kind attention and, again, your participation in all the chats and the comments and also in the Mentimeter poll. Thanks to the support staff. I think we don't do this enough.

So, thank you to all the support staff that's been involved in this session, in particular the At-Large staff as well. Interpreters, thank you so much for your service and the technical staff for keeping us moving along. So, thank you very much.

JANOS DRIENYOVSZKI Thanks, everyone.

MICHAELA SHAPIRO Thank you. Thanks, Justine.

UNKNOWN SPEAKER Thank you, everyone.

[END OF TRANSCRIPTION]