ICANN84 | AGM – GAC Discussion on DNS Abuse Mitigation
Tuesday, October 28, 2025 – 13:15 to 14:30 IST

JULIA CHARVOLEN

Welcome to the GAC session on DNS Abuse Mitigation on Tuesday, 28th of October at 1315 UTC. Please note that the session is being recorded and is governed by the ICANN Expected Standards of Behavior, ICANN Community Participant Code of Conduct, and the ICANN Community Anti-Harassment Policy.

During the session, questions or comments will be read aloud if submitted in the proper form in the Zoom chat pod. Interpretation for this session will include all six UN languages and Portuguese. If you would like to speak during the session, please raise your hand in the Zoom room, and please remember to state your name for the record and the language you will be speaking, in case speaking a language other than English. And please speak at a reasonable pace to allow for accurate interpretation.

I will now hand the floor over to Nicolas Caballero, GAC Chair. Thank you, and over to you.

NICOLAS CABALLERO

Thank you very much, Julia. Welcome back, everyone. I hope you enjoyed your lunchtime in the beautiful city of Dublin. I have the pleasure of introducing our guest speakers today. We have Edmon Chung from DotAsia. We have Jo-Fan Yu, and I hope I'm pronouncing your last name well, from TWNIC. And I don’t see Mr.

McDermott. Well, I assume he will be arriving soon. Thank you so much. There we go. Welcome. Take your time, no problem. And our GAC topic leads for this very important topic for us, which is DNS Abuse Mitigation, are going to be Martina Barbero from the European Commission, Susan Chalmers from the USA, and Mr. Tomo Miyamoto from Japan. So, thank you again. I'll give the floor now to Tomo precisely, who's going to walk us through—who's going to give us an introduction and a reminder of objectives and how it will be related to the GAC annual plan, and so on and so forth. So, over to you, Tomo.

TOMONORI MIYAMOTO Thank you very much, Chair. Welcome to the GAC DNS Abuse Mitigation Session. I'm Tomo Miyamoto from Japan. This slide, okay.

Here is the agenda for this session. After a brief introduction for me, we will have the host country presentation from Declan. And we will now learn the effort of DNS Abuse Mitigation in Ireland. And then we will review the update on PDP, on DNS abuse and we will also cover the effort against DNS abuse outside the ICANN remit. And Jo-Fan and Edmon will have a presentation of Trusted Notifier Program led by TWNIC and DotAsia. Next slide, please.

Okay, thank you. Let me introduce some background on DNS abuse discussion. As you know, dealing with DNS abuse is quite important for the GAC. And I guess, many of the colleagues here are struggling with this problem in each country. And it's also a big issue for

stakeholders as we see in this ICANN, many sessions regarding to the DNS abuse. So, based on the ICANN contract, the RA and RAA amended last year, 2024, gTLD registries and registrars must respond to reports of actionable DNS abuse report.

What we need to note is that the scope of DNS abuse in ICANN definition is fairly limited. Namely, malware, botnet, phishing, pharming, and spam as a delivery mechanism. I know that many countries have various issues on abuse and it can be [system], crypto fraud, and cooperation with law enforcement maybe. For example, in Japan, the issue of manga piracy is a huge problem, which gains several hundred million accesses per month regularly. However, they are out of the policy scope of ICANN.

The GAC takes a two-pronged approach in this situation, as revealed in the annual plan that we discussed earlier this week. First, we advanced the policy work which is based on the current ICANN definition on DNS abuse. What we need to take care of is the timeline. We want to implement a new policy before the delegation of new gTLDs. And second, we will work on capacity building on DNS abuse mitigation, including sharing best practices. And that may assist the advanced voluntary initiative taking each jurisdiction with extended communities to deal with issues of various DNS abuse, taking a variety of measures should be necessary. Next slide, please.

And some of you might remember this chart. This shows the landscape of the relevant communities. The green square shows

the scope of ICANN contract, and it is fairly limited, as I said. And the definition is [inaudible], and only the relations between the ICANN and contracted parties. However, it is contractually binding, so it is strong. So, what we aim here is to implement effective measures in a timely manner. In other words, before the delegation of new GTLDs.

And of course, we need to consider measures in the blue square or red square in the broader communities between registries and registrars and the ccTLD operators, and collaboration between extended partners. Next slide, please. Can we go to the next slide? Thank you very much.

This is the path we made so far towards the current PDP discussion. This is in the ICANN remit. And to implement the policy [inaudible], we discussed the narrowly scoped PDPs. And this slide shows some key elements. First, in November 2024, I think, many of us are reminded, but we had the informal report, informal study. It suggested some factors that drive DNS abuse, such as free API connected with bulk registration as a positive factor. And some negative factors like additional verification of contact information.

And in May this year, we had NetBeacon issued a white paper on PDP for DNS abuse litigation. As the slide shows five elements were suggested by this white paper. And based on these inputs, the GAC discussed our advice on initiating narrowly scoped PDPs on DNS abuse mitigation. In the last ICANN meeting in Prague, we issued consensus otherwise, and prioritized measures against bulk

registration, and associated domain checks to encourage the process. We will delve into this point later in this session. Next slide, please.

So, let's move on to the next part, host country presentation. We welcome Mr. Declan McDermott from .ie, the ccTLD operator of Ireland. We will learn .ie's effort on tackling illegal and technical abuse. So, thank you, Declan. The floor is yours.

DECLAN MCDERMOTT Thank you, everyone. Hi, everybody. My name is Declan. I'm the policy and regulatory affairs manager for the .ie ccTLD. I have a policy background. I am not a technical person. This will not be a technical presentation. If you do have technical questions on how we mitigate abuse, I ask that you mitigate your expectations of me. But in all seriousness, though, if you do have any questions for me, just find me afterwards. And if I don't know something, then I will strive to find an answer for you. So next slide, please.

The .ie registry has managed and run the .ie domain name since 2000. We actually just had our 25th anniversary several months ago. I think the main takeaway that I did want to emphasize to everybody is that it has very low volume and very low rates of abuse. Its total database is about 300,000 registrations, domain name registrations. Most of those domain name registrants are from natural persons. I did ask our friends at NetBeacon for a quick snapshot data of what abuse figures look like for .ie. And they gave

us some information for the latest complete month from August, where they found one detected case of phishing, I believe.

So, the abuse rate is quite low, as well as the volume. As well, for a good measure, looked at the DNS Research Federation, where they also indicated that our abuse rate was something like 0.05 percent, and in the last 365 days, there is just upwards of about 100 detected instances. So, the main takeaway from that is, I would say that it's somewhat of a smaller registry compared to some other ones. And it also has very low rates of abuse, which my understanding is quite typical among ccTLDs. Next slide, please.

So .ie also has somewhat of a unique requirement that we call a connection to Ireland. Since its creation, the .ie domain name has been intended to be used by individuals or organizations with a connection to Ireland. So, this generally falls into about four different categories. So, these are either individuals who are based or resident in Ireland, or this could be citizens of the island of Ireland that are living abroad. Or this could be organizations that are based in Ireland with, for instance, with an Irish CRO number, or an organization that is based outside of Ireland, but can prove that they are providing goods and services or selling things to Ireland. So, that's generally the four categories that we would consider a connection to Ireland. To my understanding, I don't think it’s somewhat of a unique requirement. I don't think any other registry has a connection to Ireland sort of requirement. But anyway, next slide.

So, when it comes to abuse, I wanted to say that .ie has somewhat of a broader view when talking about it than the conventional ICANN definition of DNS abuse. Internally, we tend to divide that into three categories. So, that would be technical abuse, which includes things like malware, phishing, and botnet. So, that would be more of what I think when most people would call DNS abuse. But then we also talk about content abuse. So, that could be like illegal practices or illegal content like fraud, for instance, or horror cases like CSAM. And then there's also registration abuse, which could be things like registering things in bad faith.

However, the main thing that I wanted to kind of convey though is that, yes, definitions are important. But in my personal view, what is super important is that we have different measures that can appropriately and proportionately respond to situations. So, for example, it is not appropriate for a registry to start determining what's a crime or what's illegal or what's bad faith. However, if there is, for instance, a judge or a regulator or an adjudicator that says that is illegal or that is bad faith, that there should be measures in place that we can respond to those in a way that's necessary and proportionate. Next slide, please.

So, I think I quite like the acronym ATOM, Having Appropriate Technical and Organizational Measures. This is just a very high-level, non-exhaustive list of the different measures that we have at .ie. Again, with this main point is that I firmly believe that you need to have both those organizational and those technical measures involved. I don't think that there is any one silver bullet. There's no

one control that can really prevent everything. Things like domain name suspensions or at the government level, for instance, laws and regulations. We always say that these are blunt instruments, so similar to like a hammer. They're very necessary when needed. They're very useful when needed. But for instance, if I'm trying to build a birdhouse, but the only thing I'm using is a hammer, it will be a very crappy birdhouse.

So, the point is, you sort of need this collection of different tools and instruments to kind of have a very comprehensive approach, if you will. So, some of you from, I guess, the cybersecurity world or with a cybersecurity background might recognize things like preventative, corrective, and detective controls. I actually like to use another framework from another policy lifetime that kind of actually comes from public health. Next slide, please.

So, in the world of public health, if we look at the term prevention or mitigation, prevention is about using appropriate interventions to stop something bad from happening to the health of a community or an ecosystem or a population. That's essentially, at its fundamental level, that is what prevention is about. You are having an intervention that is either necessary or proportionate that is stopping an adverse outcome from happening. So, it's divided into different layers. And I will note that, yes, this comes from the world of public health, but I've seen it applied to a number of different policy areas.

I've seen it in like homelessness prevention or environmental assessments. And yeah, I kind of like to use this framework when I'm thinking about the different measures and like mitigative controls. But yes, so looking at the different layers. So, we start off with primary prevention. This is addressing an issue before it becomes a risk. So, this is stopping the heart attack at 60 by being active when you're 30. You are preventing the data breach tomorrow by having data protection by default and design today.

At the organization level, this is essentially about having your policies and your good governance practices in place. At the government level, this would be looking at if your legislative or regulatory environments are helping you achieve your goal, if that makes sense. So, if your goal is to increase cybersecurity, are your laws or regulations forcing things like registrars to do things that are not safe or that are less secure? If the goal is to improve data protection, are there different regulatory or policies that are in place that are forcing organizations to do things that are not protective of personal data?

So, ultimately, with primary prevention, it is about looking at the broader picture of your regulatory environment and seeing if it's actually helping advance the goals and if it's using an appropriate instrument or if it's just sort of, there ought to be a law sort of approach.

Secondary prevention is a little closer to the issue. This is about stopping a threat that's imminent or in its early stages. So, in the

health example, this is about early stages of a disease. There's a disease, symptoms have been detected. This is about detecting that problem and then having rapid response to sort of stop it from getting worse. So, for instance, in its context, if a website is compromised and it's being used for phishing, are there systems in place to detect that? Are there processes in place to respond to that? If there's a DDoS attack, for instance, is there something to—for instance, like Anycast, is there a control to sort of stop that imminent attack?

Tertiary prevention is about something has already happened. Like the hospital is being ransomwared. Something legal has gone through. Something has happened. It's about harm reduction. So, in a case like this, for instance, it could be what controls are there to correct or to stop further harm from happening. So, in a domain name context, for instance, this could be in very extreme situations like takedowns or domain name suspensions, if it's found to be necessary and proportionate.

But the last one that I find that often people miss even in the public health sphere is called quarternary prevention. Quarternary prevention is about preventing inappropriate interventions. So, if secondary prevention is about preventing false negatives, quarternary prevention is about preventing false positives. It's about intervening when you don't need to intervene, or intervening in a way that is disproportionate to the situation, or intervening in a way where there's like an imbalance with fundamental rights, or in a way that just is not actually even addressing the main issue. So,

this is about having the measures in place to prevent that. That could be policy reviews, challenge functions, regulatory impact assessments. But yeah, next slide please.

So, with .ie, just to kind of emphasize then, so like with .ie, we do have these different measures in place. So, we do start off with like the broader policies and the practices and then we get into these more specific technical measures. But the main point I wanted to kind of get across is that while each of them individually might do different things, they all ultimately work toward the same goal, which is .ie being secure and trusted. Next slide please.

So, as a brief example of one protocol that we have in place, and I think that it does speak volumes to—we actually have a very good relationship with our regulators and with our government departments, colleagues as well. And I feel like things like the regulatory authority protocol that we have is sort of an example of that. So, this is a protocol where if there's a regulator or a law enforcement agency that has flagged an issue, say someone is calling themselves an architect when they're not actually an architect, and then that violates a law. And the regulator for architects go, this Art Vandelay guy is not actually an architect, so action needs to be taken against it.

So, we will have something called a due diligence check where we are examining the request, we're seeing what exactly is it that they're requesting, have they provided a legal basis? Have they provided enough information for us to sort of make a decision if on

what they're requesting is necessary and proportionate? Have they given the necessary information that the law says they have to provide for these things? And then if it's found that yes, this is like a proportionate request, what generally happens is the registrar and the registrant are then notified of it.

And if it's not an urgent situation, then the registrant is given the number of days to address the issue. They're given the contact information of the regulator so that if they have questions, they can take it up with the regulator because ultimately what we want to avoid doing is putting ourselves in a position of judge where we're going, oh yes, this is harmful content, it has to be taken down. What we are doing is sort of acting more of as a conduit where the regulator has an issue and we are putting them in touch with the individual that they have an issue with and giving them a chance to address the issue.

So, at the end of the time period, if the regulator comes back and says that it's an unsatisfactory response, then depending on the situation, then we can take corrective action and that could go all the way up to, for instance, like a domain name suspension. But I would say that almost all of the time, what generally happens is that the registrant goes, “Oh, I didn't know,” and then they make a quick change and then everything is good.

I will note that in, for instance, if there is a severe or an urgent or a nightmare scenario, we have emphasized and our regulators do know and law enforcement also knows that if they want something

taken down immediately, they have to go to the hosting provider because while we can suspend domain names, if someone has the knowledge of the IP address, that doesn't actually remove the content from the internet, though someone who knows the IP address can still access harmful content. So, regulators and law enforcement know that if they want something taken off of the internet, they need to go to the hosting provider.

However, if for some rare reason, to my knowledge, it's never happened, that they need something urgent taken down and that's not working, then they can come to us to ask, what can you do about like the domain name, so we can at least make it difficult to get to. To my knowledge, and knock on wood, that hasn't happened. Next slide, please.

So, one last framework I also enjoy from Public Health that I'll leave you with, and I find it's really helpful when you're assessing different tools or interventions that are possible. I see, yeah. So, it comes from the world of Public Health, it's called the ladder of intervention, but essentially, this will just take the different ways that a government or an organization can actually intervene, and it lists it in order of invasiveness. And the idea is that the more invasive it gets, there has to be more justification. There has to be proportionality to it.

So, it starts off at the very bottom, is essentially do nothing. In Ireland, in every regular, almost every regulatory impact assessment that you'll see, do nothing is sort of like a default

option that you have to compare against. And it's sort of like the onus is on the government of why something has to be done. Moving forward, you can provide intervention, provide information. So, this is how you can protect yourself against DNS abuse. This is how you can protect yourself against phishing. Moving forward, could be enabling choices.

So, as a registry, we enable choice of things like registry lock or DNSSEC, but we don't necessarily force people to take that. Shifting defaults is that you're essentially taking your preferred option and making it the default option. So, by default, we will not publish a registrant's personal information on the WHOIS, unless for some reason they explicitly go, yes, I want you to do it. And they have to have their explicit consent to do that. But then we start getting into more nudge theory, like behavioral economics.

So, incentives, the government wants organizations to have better cybersecurity. This is the grant fund to enable that. The flip side of that is disincentives of, they want better cybersecurity, so they have increased audits for organizations that don't have an accreditation like ISO or something of that sort. Restricting choices, this is essentially you have choice A, B, and C, but you must choose one.

So, for EU registries, this is you must verify registrant information from NIS2. How you do that will be determined by what member state you are in. But then the last one is eliminate choice. If there is CSAM, you must report it. There is no choice. If there is a court order

that says you must take action against this domain name, there is no choice.

As an example, for instance, in Ireland, we have something called an access blocking order that a judge can request. And I don't know all the requirements off-heart, but essentially, it's saying, if there is a life and death situation, if it is not unduly overriding their fundamental rights of an internet user, and if the judge is convinced it's necessary and proportionate, then they can order an access blocking order. I believe, also only for a maximum of 28 days. And then you have to reapply for another one.

But essentially, all that is to say is that they try to make it so that the most invasive option, eliminate choices, has to be for the most extreme situations. Because while these tools, or combination of these tools might be useful, if they're not proportionate, it could actually have adverse effects. So, next slide please.

So, the main key takeaways I just want to leave with everyone here is that effective mitigation, no one tool is enough. You do need appropriate technical and organizational measures. Interventions have to be appropriate. They have to be necessary and proportionate. In the case of .ie, we have found that meaningful collaboration between regulators, registrars, and the registry is very helpful in these situations. And lastly, it is very important to prevent overreach and inappropriate interventions. Thank you.

TOMONORI MIYAMOTO: Thank you very much, Declan, for your presentation. We'd like to accept one or two questions for the sake of time, but do we have any questions? Well, I see no hand right now, so I'd like to—yeah, Bangladesh, please.

DR. SHAMSUZZOHA: Thank you. This is Shamsuzzoha from Bangladesh. Thank you for the very, very good presentation [inaudible]. And it's quite encouraging to see how the constructively the ccTLD operation is going on in Ireland. I have two very quick question. The first one is regarding the regulatory authority protocol. So, the way you explained it, it seems that it's mostly reactive. That something is coming from any of the regulators, but in the proactive measures to mitigate the abuses, for example, what should be the process and the documentation that should be checked for registration and so forth? So, is there any provision for the regulatory authority to intervene or not? So, this is one thing.

My second question is that, to check the proportionateness of the system, what are the measures are taken how they are proportionate or not? What is the review mechanism that .ie is taking maybe periodically, or is there any mandated system, or is like simply there is a good faith or self-initiated process? Thank you.

DECLAN MCDERMOTT

Thank you. So, I'll answer the second question first. So, we have various different policy review kind of mechanisms. So, we have an external multistakeholder policy advisory committee made up of our different registrar. Our government has a permanent seat on it, and there's also different local organizations that are involved in Ireland's internet community. So, that's one mechanism where they can review the policy changes, or any policy changes that are substantive ultimately have to kind of go through the policy advisory committee. So, they're making sure that it's not unduly disadvantaging anyone, or that it's in line with .ie's values.

And as well, there's also the option that if there's like a significant policy change, then it also can go to public consultation, which we've done in the past when we've had some substantial policy modifications. But on your first question, I think ultimately, it is going to depend on the specific context. So, for us, just speaking for .ie, it is a smaller registry. It doesn't make sense for us really to kind of have any proactive content moderation really, and I'm not even sure that we would necessarily be even allowed to with our national legislation.

But I think it ultimately is just going to depend on what the regulatory context that a registry actually exists in, and then finding the balance of how much exposure to risk there is. Because if we look at the stats of how much actual abuse happens within .ie, the exposure to risk is quite small, yes.

TOMONORI MIYAMOTO Thank you very much for the questions. So, let's move on to the next part, the update on PDP [inaudible]. So, over to you, Martina.

Thank you very much, Tomo. And I'll go as quickly as possible through this very important topic because we're already behind on time. If we can go directly to the next slide.

Thank you so much. So, Tomo already mentioned that in Prague, the GAC issued communicate text advising the board to urge the GNSO to undertake preparation for narrowly scoped PDPs. This was followed by the preliminary issue report on policy development process on DNS abuse, which was released in September. And in the public comment that followed, the GAC submitted a response, and I will just give a few indications of what we highlighted from the GAC response.

But what you need to know from the issue report, in case you haven't read it yet, is that, it suggests prioritizing as topics for DNS abuse work, three gaps, unrestricted APIs, associated domain checks, and domain generating algorithm or DGAs. And the report argues that the first two topics, so unrestricted APIs and associated domain checks, are fit for policy work, while domain generating algorithm could be addressed, not necessarily through policy work.

So, in its response, the GAC, if we go to the next slide, we'll see it, offered support for the two topics picked for policy work, so unrestricted APIs and associated domain names. And of course, the

GAC is always very pragmatic, so we prioritize the approach that will lead to results in the most effective and fastest possible way. We also, as a GAC, highlighted the issue report contains a number of other gaps that needs to be addressed, because while the two PDPs that will probably start will be significant advancements in addressing DNS abuse, DNS abuse is a very broad and multifaceted topic, and those PDPs will not be enough to end DNS abuse, unfortunately.

So, the other gaps that are identified in the issues report needs to be addressed as well, and the GAC highlighted that some in particular are of importance, and those are listed in the GAC response. We also highlighted that the GAC would like to participate in the PDPs, but for that, we would need more information on the working methods, and we offered the possibility to have alternate participants on top of the participants, because this is something that the GAC had in other PDP process and worked very well. So, if we go to the next slide.

Yesterday, there was a GNSO-led community session on the PDPs, on the prospective PDPs. I just wanted to very quickly highlight some of the discussions that happened. And in terms of the structure of the PDPs, there seemed to be some alignment on the idea of having two PDPs instead of one only, although a lot of the details in terms of the charters and the functioning were not addressed specifically in yesterday's discussion. There was also some support from some community to maybe think twice about

addressing domain generating algorithm as a non-PDP topic. Some communities would prefer to see a PDP on that matter as well.

And then on the two specific topics at stake, so unrestricted APIs and associated domain names, there were some discussion about the problem definition in relation to unrestricted APIs. In previous GAC comments and in general, sometimes we speak about bulk registration rather than APIs, and the SSAC that we will see later today, they seem to argue that APIs are just one of the way to register domains in bulk. But if we address only that, we might not solve the issue that we hope to see addressed.

And then on associated domain, this is a topic that seems to be relatively simple to address although it's important to maintain the right balance between clarifying which checks are performed on the basis of which characteristics, whether it's the identity of the registrants or the payment method, maintain transparency versus allowing the registrars in particular to have an approach that does not provide abusers with all the information they need to avoid the abuse. So, this is important. So, if we go to the next slide.

This is very, very quickly to suggest that if those PDPs were to go ahead, as it is most likely at this stage with the refined charters, the GAC would participate in them and building on previous experience something that works quite well. Oh, sorry, I need to slow down. I'm trying to be fast because we need to catch up, but not too fast. Something that worked in previous policy development process was to have a small team, because as you know, in policy

development process, there will be one or two representative from the GAC plus potentially alternates if the charter is modified as the GAC requested, but not the entire GAC can participate. And we know that DNS abuse is a topic that is very, very important for many of you.

So, one way to make sure that everybody who is interested in participating can participate and make their voice heard is to have smaller groups, what they call the small team or small group, that prepare a bit the work of the PDP and in which whoever is interested can sit and exchange with the GAC representative to the PDP. So, these worked very well for registration data and we think it could be an approach as well for these PDPs that are coming up. If we go to the next slide.

So, this is my last slide and I'm hoping that we can have a bit of discussion here. So, we have three questions for you. The primary question for today is whether based on the discussions we had in this GAC room, but also yesterday with the community, there is any further message that needs to be highlighted towards the GNSO or the broader community with respect to the upcoming PDPs, in terms of the structure of the PDP or the topics or both, and also, if you can already let us know potentially whether you would be interested in being involved in the PDP effort or the small group, that would be interesting for us to know already who is really motivated to take up this work.

The second question regards the additional work that needs to be done on DNS abuse going beyond the PDPs. So, we have a list of potential topics that needs to still be addressed, and if there is any message to be passed to the community on that, beyond what we already mentioned in the public comment from the GAC, that's also a moment for you to raise this point.

And final question, of course, as a broader general question, if there is any other matter that we need to discuss in terms of DNS abuse based on the preliminary issue report, please, this is also a moment where you can bring up whichever other topic you would like to see reflected in the discussions. Nico, I give it back to you in case you want to moderate.

NICOLAS CABALLERO Of course, thank you so much again for that very detailed and nuanced presentation, Martina, European Commission. Thank you so much for that. This is a very good moment for our distinguished GAC colleagues to intervene us regarding any of the three questions there or any other thing, of course. So, I have Germany, please go ahead.

RUDY NOLDE Thank you. Rudy Nolde, GAC Germany for the record. First of all, thanks to you, the topic leads, for this excellent presentation, and also for all your engagement in the last month and years. For Germany, DNS abuse is definitely a top priority in ICANN, and we

would be happy in any capacity where we are needed in GAC to engage certainly in a small group, and we are flexible where we need it most.

On the second question, remaining policy gaps, I would hope, that's more general, I would hope that the coming PDP or PDPs would serve as a successful blueprint for further work, so we narrowly scope a topic and then we move swiftly. So, I hope there's also an understanding in the GNSO that once we have tackled these two topics, that we have more in the pipeline, and we won't say, let's wait two years until we see what is happening here, but we succeed with other topics.

Yeah, these are probably my two comments on this. Thank you very much.

NICOLAS CABALLERO Thank you very much for that, Germany. And by the way, I would assume in this case that Germany volunteers for part 1A of the question? No, I'm joking, I'm joking. Thank you. Thank you, Germany. I have India and then the USA. India, please go ahead.

SANTHOSH THOTTINGAL Thank you, Chair. This is Santhosh for the record. So yes, we are interested in being involved in the PDP work, and we support the launch of the narrowly scoped PDP, mainly to address the two high priority issues, which has been identified in the preliminary issue

report mainly on the unrestricted bulk API access and the lack of associated domain checks.

So, these are two issues basically directly enable systemic abuse through large-scale automated registration. So, we aligned with the ICANN83 consensus advice targeting for a targeted PDP action on these matters. So yeah, thank you.

NICOLAS CABALLERO Thank you. Thank you, India. Well noted, I have the USA next.

SUSAN CHALMERS Sorry. I'm happy to chime in. On the second question, I just recall our discussion from earlier today with the ALAC on transparency and reporting, where it was noted that reporting requirements by the contracted parties are not presently in the contracts. I believe there is a requirement to retain records of abuse reports received by the registrars, for example, but there's no kind of public reporting requirement for how many abuse reports one has received and how they've responded.

I note that because during our cross-community discussion, which was a great session, by the way, there was a question about compliance for the associated domain check proposed PDP and how compliance could be effective. It would seem to me that if there is also a transparency reporting requirement that could assist with compliance—so, that's a very technical intervention, but I think also regardless, it would make sense for compliance. And we

also indicated this in our GAC comment to be engaged in the discussions from the very start. Thank you. Over to Finn.

NICOLAS CABALLERO Thank you very much, USA. I have Denmark next.

FINN PETERSEN Thank you very much. Finn Petersen from Denmark for the record. Thank you very much for the presentation. To the question number one, which was also mentioned from the [inaudible], this on API might be too restricted, and we used to use the word bulk registration at least here in the GAC, and perhaps it would be, even though it's a narrow scope PDP, to try to investigate what other methods than IP. I could be within the scope of this narrow-defined PDP, so we are not trying to solve the wrong problem, but actually got a PDP and the outcome of that to be implemented which are effective.

On the other, the domain name registration or associated domain name, I, of course, see that the checks which are going to be carried out is difficult if you reveal them beforehand. On the other hand, if there's no guidance on what to do, then the question is, how can compliance actually look into whether they are fulfilling the PDP. So, I think that's another question to be looked into and how do we, on the one hand, not give the transparency to the back actors, but on the other hand, give the necessary instrument for ICANN

compliance to look into how this implementing PDP will work in the future.

From Danish side, we will also be happy to contribute to the work as an associated member or whatever you are calling them. Thank you.

NICOLAS CABALLERO Thank you very much. Well noted, Denmark. So, that's regarding 1A, I would assume. Is that correct, Finn? Thank you so very much. So, the floor is still open. I have the European Commission next.

GEMMA CAROLILLO Thank you very much, Nico. Gemma Carolillo for the European Commission. I think, first of all, to note that we have achieved a lot of progress in the past few years. So, we just not continue discussing about DNS abuse, but collectively, because of course, this is not the GAC alone that can do anything actually on this matter. But as a community, we are going a long way, so just to express satisfaction.

And as regards the question number two, because question number one, I'm afraid, there is no way to escape it. I mean, the commission is already part of the topic leads, but I wanted to echo the comment from Susan from the United States, and Finn has also referred to that. This is not because we are brilliant, but the GAC has already at the time of the contract amendments raised the issue of transparency, of the fact that this could be a very important

topic, and that this could have been already addressed at the time of the contract amendments. And we have prioritized it as remaining policy gaps, because this is also part of the issue report.

Two other elements that have been highlighted in the issue report such as the use of proactive preventative measures, Nico, you will be very happy about the reference of the use of detection algorithms. So, this is recommended as another work stream. And then there is part of the issue report referring to the need to address accuracy of registration data, and particularly the validation aspect. Good news is that, if I understood correctly from the chair of the GNSO small team on accuracy, they intend to pass on this work now to the GNSO small team dealing with the DNS abuse, so that there should be activity around this important topic. Thank you.

NICOLAS CABALLERO Thank you so much for that, European Commission. Indeed, I'm happy about the issue, about the algorithm, but also worried because please remember, the bad guys also know about these tools. And I'm not talking about ChatGPT or generative AI, LLMs. I'm talking about very sophisticated algorithm using random forest and clustering and many other. We talked about that the other day. I'm not going to get into details, but you're right.

So, the floor is still open. Any other comment or question before we move on, for the sake of time, we need to cover some other issues as well. So, seeing no other hand up in the room or online, I'll give

the floor now to Susan, who's going to walk us through the issue of Trusted Notifiers Program and a Q&A in that regard. Susan, over to you.

SUSAN CHALMERS

Thank you, Chair. So, now we'll take a bit of a pivot. As my colleague, Tomo, explained earlier, the GAC's strategic objectives on the subject of DNS abuse are organized into two general categories. First, we've been working to advance policy work at ICANN on DNS abuse and presently in this regard, we are encouraging the PDPs to move forward. But secondly, we have a capacity building section.

And so, the topic co-leads have been working too, and will continue to work to provide resources to GAC representatives in order to build capacity on the subject of DNS abuse in general. If you'll see in Section 4.7, one of the ideas was to provide information on what are referred to as Trusted Notifier Programs. So, if we flip to the next slide.

A familiar one. You'll see that Trusted Notifier Programs can be used to address DNS abuse activities that are outside of the remit of ICANN's contracts. And so today, we are very lucky to be joined by representatives from DotAsia and TWNIC all the way on the other side of the [inaudible] to present on their Trusted Notifier Program. So, I'd like to turn it to them. Please.

EDMON CHUNG

Thank you, Susan. Edmon here. And I chatted with Jo-Fan and I'll go first and then pass it over to Jo-Fan. Thank you for having us here. This is a topic that is dear to my heart. I'll come back to a little bit of the history there, but I think it is a very important part.

And if you go to the next slide, you'd see it is my version of, I guess, Tomo's and Susan's slide to identify that there are abuses happening, DNS abuse happening beyond the ICANN remit. And this is a very important part because it happens in different components in the network. And that's why focusing only on the ICANN remit is probably unsatisfactory.

If you go to the next slide, that gives you a different view, which I think, echoes, I think, Declan's earlier discussion about the broader view of abuse. Here you can see that this is how, really, DotAsia and us see it, is that there is the larger cyber abuses, and then within that, there's a smaller chunk that we call DNS abuse. And then in further smaller part is actually abuses that are appropriate for top-level domain registries to deal with. And part of it is within the ICANN remit, and in fact, part of it is beyond the ICANN remit, including CSAM and other issues. And that's the part where I think is interesting and important to also look at, and doesn't have to end up with the ICANN PDP.

And one of the great examples, I believe, if you go to the next slide, is our work with DotKids. This started just before the last round, and we knew very clearly at that time that the same policy for DotSex is probably different than the policy for dealing with abuse

with DotKids. And herein lies an interesting aspect, which is how do registries—sorry, rewind a little bit. I should say that registries start with the ICANN remit as the baseline for dealing with abuse, but we don't stop there. And there are certain situations that definitely we should go above and beyond, and DotKids is a great example.

But I also want to highlight that today, as we launched DotKids two years ago, it was a lot of the DNS abuse platforms and technologies that were put in place over the last 15 years was actually very instrumental in allowing us to do further things, to address further abuse, to even put watch lists together, and I'll touch on that. If we go to the next slide.

As I said, this is our journey started way back in 2011. You probably didn't realize that back then, we did have a forum on DNS abuse that was probably one of the first ones that DotAsia participated in. We've gone a long way over the last 15 years.

And the last slide is where I want to talk about the Trusted Notifier. It is really, at this point, as I mentioned, we're looking at going above and beyond what the contractual requirements are, and we're starting with a registry-to-registry kind of approach. So, our Trusted Notifiers, at least the ones that are formalized, are other ccTLD registries, and we will also probably welcome other gTLD registries as well, but I'll touch on why ccTLDs are so important part of it.

The reason why for registries is because we want to maintain a similar level of sensitivity to the bluntness of domain suspension,

because the ability for registries to actually act essentially as a suspension of domains has a larger effect, and we want similar sensitivities from different registries so that they would be able to look at that and pass it to us for what we call an expedited suspension. And on that, what happens actually, the two pilots that we have built right now with .TW and .UK and Nominet is that we have a trusted channel for communication.

It's actually very simple. It's a dedicated email with shared keys, so that we know that whoever's sending it to us is a trusted source, and we request for a certain format of due diligence, and we can act quickly on it. That is what we're doing, and we're hoping that from here and outwards to invite many other ccTLDs to come join us. I could report a little bit. In the last few months, well, last year or so, we have been putting this together, and then the last few months, it is becoming to be in action, and there are domains that we are receiving notification for.

And one of the reasons we found is that, I think you might know about this, but we're seeing it in real situation, is that sometimes phishes are dedicated to particular regions. If the phish is dedicated to Taipei, for example, some of our monitoring systems don't pick it up, but that could be picked up by our colleagues in Taiwan, and they can actually send us the notification, and we were able to deal with this. And this is one of the reasons why we're very excited to work with different ccTLDs, because essentially, the kind of monitors or the kinds of things that globally we can do is

probably, there are things that we will miss from phishes or attacks that are very directed to certain geographical locations.

And with that, really, I wanted to highlight that, we are exploring other aspects as well, again, beyond the ICANN remit. We're starting with the ICANN definition of DNS abuse, but we are interested to expand the Trust Notifier Network to cover other types of abuses as well, and that's where we invite other ccTLDs to work with us, and through the ccTLDs, maybe to connect with the national search and response teams as well. And that allows us, again, through ccTLDs, maintaining this sensitivity at a registry level, but still try to deal with abuses beyond the ICANN remit. And with that, that's my presentation, and I guess, I'll pass it on to Jo-Fan directly, or if Susan wants to...

SUSAN CHALMERS Thank you, Edmon. Sorry, but just to take a step back, and forgive me, I should have done this before the presentation, but here we have a representative from a registry that runs a gTLD joined by the CEO of TWNIC, which administers a ccTLD, so I just wanted to point that out. I think that's very important.

And Jo-Fan, without preempting your presentation, just one question, and perhaps we can answer it later. But what makes a notifier trusted, I think, would be useful to explain at some point. Thanks.

JO-FAN YU

Thank you. I'm Jo-Fan. Good afternoon, everyone. Thank you for inviting us. I'm really happy to share, especially, I mean, from the ccTLD perspective about what we're thinking about a trusted notifier framework? Next slide, please. Yes.

So yeah, so why we need the Trusted Notifier Framework? We know that, I mean, the DNS abuse. I mean, [inaudible], I mean, really, go global. And of course, on the other hand, we have like growing, I mean, public demand, I mean, for accountabilities. So, I think now the traditional response method, usually is not fast, and also face jurisdictions, I mean, hurdles. So, that's why we need, I mean, a Trusted Notifier Framework.

But I think I also want to raise an important point from the ccTLD perspective just like you can see from this data. Actually, as a ccTLD, we receive regularly the notification from our government about the illegal website. So, this is data, I mean, for us in 2025 until the end of September. So, you can see from this data, so only less than 1 percent of illegal websites, actually is .TW. So, meaning that in our jurisdictions, more than 99 percent is beyond our capability to take any actions. So that's why we think from the ccTLD perspective, we think it's really important. Next slide, please.

So, what is the Trusted Notifier Framework? I think for us, I think it's a framework for the fast actions based on the trust, and also, the pre-agreed rules. And the objective, of course, I mean, to handle the abuse, especially serious abuse cases more efficiently, more effectively. And we also think it's important to have the core

principle to include the trust and transparency and due process. So now, the current Trusted Notifier Framework, now we collaborate with the registry and registrars.

So, like DotAsia that Edmon and also, .UK, .KR, also gTLD as well at the top, and also registrars as well. And in addition to content abuse, but now we are focused mainly on the DNS abuse, especially the phishing. So, we use SOP and also, the agreement, I mean, to negotiate with our partners, I mean, to include also the principle like transparency and due process. So, I think it's what we are doing right now. Next slide, please.

So, you can see from these slides that without the Trusted Notifiers, so we receive the intelligence from our government and also, the law enforcement, cybersecurity community and ourselves as well, and our citizens as well. And then we investigate and report. So, for the registry/registrar, then they will take another investigation again. And based on their result, then they will take some action to block or suspend, I mean, the demand. Next slide, please.

So, when we have the Trusted Notifier Framework, so you can see that, so after we investigate and then report to the registry/registrars, so they can directly use the pre-agreed SOP and also agreement with us and then take actions. So, they don't need to spend repeated, I mean, investigation efforts. Next slide, please.

So, the benefit from our view, so first, of course, I mean, it create a framework to speed up threat intelligence, and also, abuse, to handle abuse. And second, it reduce the investigation burdens of

the registrars and registries. And the third one we think is really also very important to become more proactive, because we know that phishing maybe just live for several days. So, if we can have more quick actions and have a more credible threat, so we can take some actions before they escalate. Next slide, please.

So, I also want to share our TWNIC 2025 data snapshot. So, until now we have—this year, until now we handle 51 domains in 2025. I think we expect we will have much more numbers because we onboard our partners only the second half of this year. So, we expect, I mean, more numbers, I mean, for the next year. So, 78 percent are confirmed phishing, so our partners take some actions.

And also, the response time, now in general is less than two days. Usually, it's one to two days. But we also think we said, maybe we can speed up the process by automation as well. So, I think another good thing is that, until now we have not received any appeals. So, meaning that maybe the result is good. So, next slide, please. Next slide, please. Thank you.

So, we say, what is the challenge for us? Because registry/registrar have different criteria. So, that's why we rely on the bilateral agreement. So, it leads to the problem, I mean, to scale the framework. But I think if we're next step, we still continue to expand the Trusted Notifier, this partnership. And then we also end to develop and demonstrate non-regulatory model, maybe successful model, I mean, for the industry collaboration. And we

also hope to align with ICANN and also GAC DNS abuse best practice. So, next slide.

Okay, we think the Trusted Notifier Framework is really crucial step to fulfill the shared responsibility of internet communities. So, that's why we also encourage the GAC representative to maybe to urge your ccTLD to consider, to understand a few more and even to join. So, if you have any question or interest, welcome to contact us. Thank you.

SUSAN CHALMERS: Thank you so much, Jo-Fan and Edmon for that excellent presentation. And now we'd like to open up the floor to GAC representatives to see if there are any questions. I see WIPO, please.

Brian Beckham: Thank you, Susan. Thank you, Jo-Fan. Brian Beckham from WIPO. I had a question on the first bullet point on your last slide in terms of the question of potentially different criteria for registries and registrars and scale. Wonder if there's any utility in thinking about a standardized framework to help address that question, so that Trusted Notifiers might be able to use the vetting that they've undertaken in one context across the ecosystem more broadly.

JO-FAN YU: Yeah. Thank you for these great questions. So, I think, yes, I mean, it will really be helpful if we have a platform, especially a technical platform to have this kind of negotiation or exchange information.

But I think the difficulty right now is first, I think the awareness level in this community. So, as far as we know that—although there's an increasing awareness, but still the awareness is quite low. So, how the community can formulate a standard criteria for this kind of like intelligence sharing and also take actions, I think it's still, I mean, another problem, yeah.

NICOLAS CABALLERO Thank you very much. Would you like to respond to this, Edmon? Yeah, go ahead.

EDMON CHUNG Yeah. Edmon here, just adding quickly. So, the short answer is yes, of course. And actually, DotAsia is working closely with TW on the formatting and the kind of evidential materials that is provided, so that we can expedite any kind of suspension. And we're also working with CleanDNS and NetBeacon and those organizations as well to try to come to at least a sort of like de facto standard or industry standard, not necessarily very rigid standard per se.

NICOLAS CABALLERO Thank you, Edmon. I have Japan next.

TOMONORI MIYAMOTO Thank you very much for your great presentation. And I'd like to ask about—maybe all they covered in the last slide, but what do you

expect for us? I mean, how can we or GAC members or each government can help you assist your project? Thank you.

EDMON CHUNG

Edmon here. Well, encourage your ccTLD to join us because as I mentioned, we prioritize currently with registries first because of the sensitivity in terms of takedown notices that is appropriate proportionally for domain names at the top-level registry. So, I'd like to, I guess, GAC members to encourage your ccTLDs to join us in our network.

JO-FAN YU

Yeah, I think that ccTLD actually plays a really important role. So, I think, if the GAC representative can just raise awareness and also, just to encourage them to join, I think that will be really helpful. Thank you.

NICOLAS CABALLERO

Thank you very much, Japan. For the question, any other comment or question in the last five minutes we have before I hand over the floor to the USA for some communique considerations? And I have Columbia.

THIAGO DAL-TOE

Thank you so much. Thanks so much for the presentation. My question is precisely on that. So basically, we do not, at the national level, we do not have to set up our own Trusted Notifier Program,

we can actually join other existing programs. And if that's so the case, how can we join? What is the process to do it? And even the process for acceptance of such applications. Thank you.

EDMON CHUNG

Edmon here. So, currently, we do it bilaterally because each particular ccTLD might have slightly different requirements. Oh, I forgot one thing, besides the mutual notification side, we also share data. We share basically the quarterly. We share all the suspension data to TW and we're looking for vice versa. But some arrangements might not include part of that.

So right now, it's a bilateral kind of MOU agreement between us and the other ccTLD. And in terms of the whether you need systems and so on, as I mentioned, our channel will be as simple as a trusted email with exchange keys. But behind, we have our systems. It is up to the ccTLD whether you have your backend systems or not.

NICOLAS CABALLERO

I have a very quick follow up on that Edmon. How do you share the data? What is the format? Is it CSV, comma-separated values? Is it ODF? What is…?

EDMON CHUNG

Yeah, it is just CSV and this is domain suspended and a simple code for the reason for its suspension.

NICOLAS CABALLERO Thank you very much. Susan, the floor is yours.

SUSAN CHALMERS Thank you, Chair. Just with a few minutes left, may we please proceed to the final agenda item. So, GAC members may have seen that we had circulated previously some communique consideration text just to kind of spark some thought for the communique for Dublin on DNS abuse. And at this point in time, the topic co-leads do not have any advice to recommend. We're very pleased with the advice that we're able to produce in Prague and the progress that has been made on this topic by the community since then.

So, we are considering the following for issues of importance, and I won't read them out, but you can see them on the screen. So, if anybody has or would like to suggest any additional items for the issues of importance section, that would be great. We are working on draft text right now. So, the floor is open.

NICOLAS CABALLERO Thank you very much for that, USA. So, as Susan correctly pointed out, the floor is still open. If you have any other ideas, as usual, any good idea is always more than welcome. So, before we wrap up, anything you would like to add? I don't see any hand online, and I don't see any hand in the room, which means that we're basically in agreement.

So, thank you so much for that. We don't need to extend. We still have two minutes, but we don't need to extend the session. Thank you so very much. We're going to have a coffee break now. Actually, yeah, it's a 30-minute coffee break. Please be back in the room at 3:00 p.m. sharp. Thank you very much.

[END OF TRANSCRIPTION]