ICANN85 Mumbai | CF – ccNSO: Joint Session with GNSO RySG on Abuse
Wednesday, March 11, 2026 – 13:15 to 14:30 IST

CLAUDIA RUIZ

Hello and welcome to the ccNSO Joint Session with the GNSO RySG on abuse. My name is Claudia Ruiz and I, along with my colleague, Joke Bracken, are the participation managers for this session. Please note that this session is being recorded and is governed by the ICANN Expected Standards of Behavior, the ICANN Community Participant Code of Conduct, and the ICANN Community Anti-Harassment Policy.

Please observe the following guidelines to participate in this session. They will be posted in the chat for your reference. During the session, questions or comments submitted in chat will be read aloud if put in the proper form as noted in the chat.

Interpretation for this session will include English, Spanish, and French. If you would like to speak during this session, please raise your hand in Zoom. When called upon, virtual participants will be given permission to unmute. On-site participants will use a physical microphone to speak. Please state your name for the record and the language you will speak if speaking a language other than English. And please speak at a reasonable pace to allow for accurate interpretation.

Thank you, and with that, I will now hand the floor over to Bruce Tonkin, moderator for this session. Thank you.

BRUCE TONKIN Thank you for that introduction. So, the purpose of this session is a joint session between the ccNSO and also the Registry Stakeholder Group of the GNSO. So, both groups, as managers of top-level domains, put a significant amount of effort into reducing DNS Abuse. And there's a few activities that I can at the moment working to improve, I suppose, cooperation and also standards across the industry.

The first one of those is a GNSO policy development process at the moment, looking at, it's called associate domain name checks, but the concept is if a domain name is being found to be involved in DNS Abuse and a registrar has taken action on that DNS Abuse, the idea is that they should also look for domain names that are associated with that original domain name.

So, it could be domain names registered on the same registrar account and also check to see if there's any abuse on those names. So, I'll hand over to Brian Cimbolic from the Public Internet Registry, which runs .Org, to give an update on that policy development process.

BRIAN CIMBOLIC Thanks very much, Bruce. Hello, everyone. I am Brian Cimbolic with PIR. We are the gTLD operator of .Org, as Bruce mentioned. Next slide, please.

CLAUDIA RUIZ Brian, would you like to control your own slides? You can use the remote.

BRIAN CIMBOLIC Sorry. Boy, you guys are sophisticated here. What is this?

BRUCE TONKIN That's not a remote.

BRIAN CIMBOLIC Oh, where's the remote? Who's got the remote? I'm guessing Bruce. Bruce has it. There we go. Thank you.

BRUCE TONKIN Sorry about that.

BRIAN CIMBOLIC Okay. So yeah, I'm here today to speak to some of the policy work that has kicked off at this meeting in earnest for DNS Abuse in the GNSO space. So, there are currently two anticipated PDPs, policy development processes, kind of on deck.

The first that we kicked off, as Bruce mentioned, is associated domain check. I'll get into that in a little bit more detail soon. The second is something called, it's meant to address unrestricted access to APIs prior to a large volume of registrations.

Both of these policy development processes are really sort of trying to deal with abusive campaigns, where it's not necessarily an individual phishing domain. That is already covered in the registry agreement and the registrar accreditation agreement, but trying to disrupt abuse that occurs at scale.

When hundreds, dozens, hundreds, or sometimes they go over a thousand names, are used in a coordinated attack that are often registered by using API. So, both of these really are targeted at some of the hardest hitting forms of DNS Abuse in the DNS.

So, there's the structure of these PDPs. They are representative models. And again, there's one PDP per topic. And I want to thank the ccNSO for participating. Your thoughts and guidance in this process are really appreciated. And so, far, there's already been excellent contributions from your participants.

There was also a third item that was identified by the GNSO. And that is also something that should be of interest to the ccNSO. And that is better coordination on dealing with domain generated algorithm botnets, basically. The typical fact pattern for this is something akin to the avalanche takedown, which is pretty old now, I think 2016. But it's spread across 44, I believe.

And if Benedict's listening or in the chat, he can correct me. Anyone can correct me in the chat or at any point. But it spanned, it was not unique to gTLDs. It was not unique to ccTLDs. It was a blended mix across both gTLDs and ccTLDs. So, it's been identified that there might be an opportunity to have better coordination on dealing with domain generating algorithms tied to botnets across both Gs and ccTLDs.

There were also a number of other issues that I can post into the chat. But there were a number of issues that were identified that will be considered at some point for future policy work.

So, this is a helpful slide that I can put together on kind of thinking about the life cycle of DNS Abuse, where phase zero, you could have DNS Abuse efforts that help prevent or have registration safeguards.

Phases one and two are the detection and reporting of DNS Abuse. Phase three is the actual mitigation by the registry or the registrar. And then ultimately, if DNS Abuse makes it through all three of those first phases, there is the possibility in the gTLD space to escalate to ICANN compliance.

So, I just want to note that for the associated domain check really gets at phase three, mitigation, where the safeguards before you have access to bulk APIs, that really gets to phase zero, which is the prevention phase.

So, let's talk a little bit about the PDP that we kicked off. So, the associated domain check, as Bruce pointed out, deals, let's give a real-world example. There's a couple of real-world examples. In the US, there is a payment toll road processor called E-ZPass. And last year, we saw huge campaigns with various registrations, various strings that seemed to try and mimic E-ZPass.

So, anyone that uses a highway in the United States goes through these E-ZPass things, and so you're familiar with the brand. And so, they would have things like E-ZPassSecure-gov.TLD. And it wouldn't be one registration; it would be thousands. And so, they were often delivered via smishing, SMS phishing.

And so, these were largely concentrated in handfuls of registrars. And so, if you are only dealing with each individual domain that comes up, you're sort of playing whack-a-mole. Whereas if you have an obligation, once you make the discovery of that very first domain name, the associated domain check will ultimately create an obligation on the registrars to look to see are there any other domains that sort of fit this pattern.

And so, instead of only removing one abusive domain, you have the potential to remove hundreds all at once. So, we're working, like I said, this PDP really just kicked off in earnest. So, we're working to define triggers, scope. Of course, we want to be mindful of any impacts on human rights. And let's, one thing that's not on this slide is the timeline.

The ICANN staff came for input into the PDP, a potential timeline that I think had basically like 18 working months for this PDP. I get the sense, I won't speak for the group, but my observation was that I think we can get this done a lot faster than that.

This is a very specific question, and we all, it seems, kind of already know the answer. The question, should there be an obligation to promptly and reasonably check for associated domains related to that abuse, I think the answer is yes. So, it shouldn't take us 18 months to get to yes. And I think that actually, the first real working session of the group, there was a real spirit of cooperation and good faith.

There is a Strawman that is already for consideration in the group that would really do the laboring or of the entirety of the policy. So, we're hoping that this goal, I'm sorry, we're hoping that this PDP can be done much faster than 18 months. And I think that is it for me for now, Bruce.

BRUCE TONKIN: Thank you. Perhaps of course, are there any questions from Brian on the policy development process or the topic? Eberhard.

EBERHARD LISSE: Eberhard Lisse, .na. I'm a ccNSO appointed member to that Working Group. Excuse me. My understanding is that the Working Group should also figure out who's going to pay for it and whether it's implemented by the registries, registrars or not. And let me

finish. And I think that little thing will probably cost 19 or 20 months of the 18th UN Vision.

BRIAN CIMBOLIC: Thank you, Eberhard. And thank you for your participation. I think luckily though, those are all dealt with in a pretty tidy fashion by the charter. So, the charter scope is pretty clear. It's pretty narrowly scoped. And this is not something that actually applies to registries. The thought is that at least in unlike many of the ccTLDs in the room, or at least some of the ccTLDs in the room in which you have a direct contractual relationship with your registrants, where you enter into a contract with a registrar or at least some of you, I'm sorry, with the registrant at the same time that the registrar does, that doesn't really exist in the gTLD space.

And so, the customers are much, much closer aligned to the registrar than they are the registry in the gTLD space. So, the scope of the charter, Eberhard, does not have associated domain checks at the registry level because we won't have that same level of customer information that the registrars have. Go ahead.

EBERHARD LISSE: Quick follow up. That's not what I'm asking. The point is it's going to happen on the registrar level and everybody and his donkey is going to tell them, you're going to do it and you're going to pay for it and you're going to do it no matter what.

I foresee this is not going to be as easy as we think it is. Technically it's easy, but who's going to implement it? Who's going to pay for it? And we already see the competing interests in the first two sessions in the mornings. We wasted a whole afternoon on figuring out what consensus is and how to achieve this and stuff like this.

I am not really so sure that this is going to be as easy as you make it out to be. Never mind that, I'm quite interested and I'm continuing to remain there.

CHRIS DISSPAIN Thanks. Eberhard, thanks. Sorry, Bruce, can I just, is that all right?

BRUCE TONKIN Yeah.

CHRIS DISSPAIN Eberhard, this is Chris. Just to respond briefly to that. So, I don't think that the suggestion is going to be easy. I just think that there's a suggestion that a lot of the work has already been done and that there is a significantly large amount of goodwill in the group to get this done in a relatively speedy fashion.

PDPs take time. They take time in the ccNSO and we're all ccTLD managers. They take more time perhaps in the GNSO because it's not just TLD managers, it's a bunch of other people as well. It's a challenging environment but I think there's an understanding and

agreement across the gTLD community at least that this is important and needs to be dealt with relatively speedily.

And I just wanted to respond to your comment about wasting time at the beginning by respectfully disagreeing with you. I get as frustrated as many do at the hoops that need to be jumped through. However, the GNSO has a very specific process for dealing with its PDPs and it is different from the Cs simply because of the fact that the room, the GNSO is made up of lots of different competing interests whereas the Cs are not. And one of those is to get clear what they mean by consensus across the board. So, that work is actually very important. Thanks.

BRUCE TONKIN Thanks, Chris. Any other questions? I should point out also that there's four members of the ccNSO that are involved in the Working Group. Two people there as members. One is Eberhard Lise from .na Namibia from Africa or African region. We have Nick Wimben-Smith from Nominet. UK, European region. He's the chair of our own DNS Working Group within the ccNSO. I'm there as an alternate if Eberhard or Nick are not available.

And we also have Diego Ernesto Luna Quevedo from Colombia in southamerica.co. So, we've got quite a bit of involvement and we'll certainly, as the four of us, report back to the ccNSO on how the work is going. I'd like now to turn over to a presentation on DNS

Abuse procedures within .rs, which is Serbia. And the presenter is Dejan Dukic. Thank you.

DEJAN ĐUKIC

So, good afternoon. You can click it. Nope, that's it. Okay, thanks. Good afternoon. I'm Dejan Đukic from Serbian registry and I'll speak about our relatively new DNS Abuse procedures.

So, some quick information about our registry, just to have a picture, how big is the registry and what are the main numbers. So, we have 41 accredited registrars that are business entities registered in Serbia. So, only local companies and businesses can be our registrars.

Registration of domains is open worldwide so any users can register domain names but only registrars could be from Serbia. Our system and our policies are based on local law and we manage around 160,000 .rs and more than 3000 in IDNS relic.srb.

Abuse policies are relatively new from end of 2025 and our plan is to have awareness campaign based on those policies in this year. Also, before that we did a couple of awareness campaigns and it doesn't matter that we didn't get those policies but we are also dealing with reducing of abuse even before.

Just to be clear from policy level at the beginning, we have a general terms and conditions which is relatively old document, last changes was six or five years ago and in that document we just mentioned that we have right to delete or suspend domain if data

is not correct or if domain name is used in a way that presents as risks for domain name users.

So, actually with these new policies we didn't change our position as a registry, we just set some additional framework of policy how we react and how we prove that some domain names are malicious. We are monitoring our zone on a regular level, we use couple of scanning mechanisms at the moment, we are using couple of free tools, we also did the testing of couple of commercial tools so we will later decide which one we will use.

Also, we have couple of parties that are very often from our local level send us kind of request for checking of some registration so we receive reporting from a local level. Also, we cooperate with local authorities and I'll speak more about it later.

How we react in a situation according to new policies? We, after we receive report, we do the checking of how the user use their domain, what are the data and is it data seems like incorrect and thinks that's the first thing that we do. Also, we include our accredited registrars and they also do their part of the checking. I also mentioned couple of tools that we are using so we did additional scanning through those available tools.

We have a very good cooperation with our accredited registrars since they are obliged to react in cases like that so they need to check the data and they need to have contact with the registrants in order to find the solution and in order to check is the data

correct, is something changed or is it supposed to be changed in the future?

Also, we have at this moment good cooperation with authorities. We cannot say that it was always that good because they have a lot of cases so it's not that simple to react on every situation related to the main names but since Serbia started to implement law based on the NIS2 of our government and related ministry implemented couple of tools and improved also policies how they react.

So, in that cooperation, national search is also included and in the cases that for us is hard to get in touch with public prosecutors and his offices are national search is very cooperative in that.

Two things how we deal, two ways how we deal when we find out that domain name is malicious is suspension, that's temporary suspension and after registrar check data, check the not always content but check how domain name is used, that domain name can be returned to zone again but only if malicious content or the data is removed. Also, we have option to delete the main name temporary if there is no way to find a user or if registration is definitely malicious or if we get order from competent authorities.

So, these are the numbers for 2025. We had less than 500 cases, all of them were sold and most of them are sold in a couple of days. We also had five positive more than 200 and most of those abusive registrations was related to phishing. So, we also have malware cases, scamming legal content and other fraudulent activities.

These are numbers of what are the most situation and what is recognized malicious activities and registration. So, most of them were, as I mentioned, phishing and it's 78% in total last year.

In this slide, you can see by months, probably in October was some campaign with a lot of registration. Most of them in last year were actually in October, which is kind of funny that is October in the month of cybersecurity. So, it's strange that it's happened that month.

Now I'll show you one most extreme case of abusive registration in 2025 that represent are also very good cooperation with the public authorities in order to reduce this sort of activities. Actually, we received reports from international users, actually it wasn't in any international authority, one of the users send us this domain name. So, it wasn't also on those tools that they are using. And we did some digging also, we initiate contact with our public authorities.

At the moment, they didn't respond, but since we found out that it's very serious thing, we include our colleagues from national search and they have better cooperation with public authorities since they are part of government, but we are not, we are private foundation.

So, they had much better cooperation and reaction from them. And when they got their attention, we solve this case pretty soon, pretty fast. And this case represents selling of illegal weapons online. So, it was the thing with these domains was actually that

we as a registry couldn't react based on the illegal, based on incorrect data.

So, we checked first as we do always with our accredited registrar and he contact the registrar and he respond regularly. That's my data, everything's correct. So, you cannot suspend my domain. And after that, we had to include public authorities and after a couple of days of communication with national search and public prosecutor, we made them to release public order and we delete and firstly suspend and after delete those domains.

So, from this case, we had some lessons learned and after that, since it was the process of developing on our procedure, we decided to be more concrete with this procedure. That's the one of the reasons why we decided to implement specific procedure for reaction. Before that, we were also reacting with abuse and we were also dealing with abuse based on our general terms and conditions but with this couple of extreme cases that we had in last few years, we find out that it's very important to have some dedicated procedure that are more concrete and more clear for us and for users as well.

Thank you for your attention. If you have any questions, I'll be happy to answer.

BRUCE TONKIN If you have any questions, start with Eberhard.

EBERHARD LISSE: How many domain names have you got under management? You have about 400 cases. In other words, what's the return on investment? How much does it cost you to do this? Is it worth the financial effort financially?

DEJAN ĐUKIC: We have 160,000 domains in total and we are doing on our own. We have our team who is dealing with it. So, they're also

EBERHARD LISSE: Yeah, but how many people are working sort of in your -- how many full-time equivalents are working on this? It's just to see how much effort it is for us to implement it. How many people do we have to hire or something like that?

DEJAN ĐUKIC: One person working full-time and other people helping him, but they're also working on other stuff. So, their system administrators, they will work there much longer.

BRUCE TONKIN: Yeah, Ken.

KENNY HUANG: Thank you. Kenny Huang, Board chair of TWNIC. I'm also the first part of the question, very similar to the previous one. Actually, how

much budget you have been allocated to deal with that kind of mitigation abuse and specifically separate into two parts.

The first part should be technical abuse and that including someone reporting to your registry and someone you probably provide a general monitoring to any particular technical abuse.

Second part would be associated law enforcement agent. You need to cooperate with law enforcement agent, either domestic or international law enforcement agent. So, do you have allocated particular budget for this kind of mitigation? Second would be what would be the most economical feasible way to prevent first part technical abuse because most of the ccTLD, they are trying hard to mitigate a kind of technical abuse, but like a more feasible way and conventional way to do a best mitigation. Thank you.

DEJAN ĐUKIC

As I mentioned in the previous answer, we already had security team who's dealing with other security issues. So, they're also work on this as a part of their job. And if you ask about our cooperation with international authorities, according to Serbian law, we cannot cooperate directly to international authorities, but if we receive kind of request from those authorities, we help them to or give them advice how to reach our authorities in order to find the solution.

But it doesn't matter from who we received data or complaints, if we check our system and if data is not correct, if there's possible

way for us to react, we will react, it doesn't matter who send it. So, any user can send us any complaint.

BRUCE TONKIN Andreas.

ANDREAS MUSIELAK Andreas from NIC .IT for the record. Leon, it's a funny coincidence because you mentioned the Kraken and we call that Kraken domains at .IT. We suffered the same thing in 2025. We had a lot of registration with the name Kraken. And by a funny coincidence, I had to chat with another ccTLD from Europe and I don't want to mention that here because I don't know if he wants me to tell you the name of the ccTLD, but they were suffering the same thing with many Kraken domains.

So, probably when you're talking about you can't collaborate with international authorities, we really need to think about to collaborate on a TLD level because we suffer exactly the same thing. It's changed now, but 2025 was really a peak and we still see that Kraken domains are going to register under .IT. So, just for your information because it's a funny coincidence.

BRUCE TONKIN Yes, Brian.

BRIAN CIMBOLIC: This is Brian from PIR. Actually, Andreas, I was about to raise my hand to say the exact same thing, not that it was in IT and to shame you, but no, in org we had the exact same thing. And actually, there's a third. So, if you've dealt with Kraken before, you've dealt with, what was the other one? Mega, there's a third competitor called randomly trip scan. It's usually the word TRIP in English, TRIP-Scan. And they are all these market plates and they seem to come in batches by the dozen across different TLDs. It's very persistent. So, be curious if anyone else is experiencing this too, but it was very much a whack-a-mole where we would suspend the domain names as well. And then a week later, another batch popped up.

BRUCE TONKIN: Thank you. Dejan, in the context of the associated domains, policy development process, did you ask the registrar to look for any associated domains for the ones that you identify?

DEJAN ĐUKIC: We always use RASMAN to check all suspicious domains when you find out. So, they're included in the process every time.

BRUCE TONKIN: Okay, thank you very much, Dejan. The next presentation is from Mohamad Shidiq Purnama and it's related to the IDADX and collaborative move with TNNN.

MOHAMAD SHIDIQ PURNAMA Yeah, thank you. Maybe you can help. Yeah, you can help me to share the screen. Good morning or good afternoon and good evening, everyone. Thank you to organize for giving me the opportunity to speak in this session. My name is Mohamad Shidiq Purnama. I am Vice Executive Director of PANDI. PANDI is a registered operator for Indonesia that ID country called top-level domain. I was actually planning to attend this ICANN meeting in Mumbai in person.

Unfortunately, due to organizing a visa process, I'm unable to join you remote. So, I just joining you remotely today. But I'm very glad and I can still be part of this discussion because DNS Abuse mitigation is something that affect all of us in DNS ecosystem.

Today, I'd like to briefly share how PANDI approach abuse mitigation in the .id namespace particularly through two initiative. The first is IDADX. IDADX is Indonesia Domain Name Abuse Data Exchange. You can visit the domain name in IDADX.id. And the second, our collaboration concept through Trusted Notifier Network.

Before diving into abuse mitigation, let me briefly introduce about PANDI. PANDI is a nonprofit organization established in 2006. And we began managing the .id namespace in 2007. Later in 2013, the .id domain received a delegation from IANA. So, PANDI give a data delegation from 2013. Today, the .id domain name has grown to

more than about 1.4 million domain name under management. This data as of December, 2025.

PANDI operate under multi-sectoral government model where our member represents government, industry, academia, and independent stakeholder. And we believe this multi-sectoral model approach is essential because especially when we're dealing with a complex issue like DNS Abuse. And we have some registrars. We call two types of registrars. The first is special registrar. The special registrar manages like government, military, and special script. And other type of registrar is commercial registrar.

Next slide. Like many other registries, currently we see different type of abuse occurring in the .id namespace. During 2025, PANDI identified about 26,000 abuse related report with the .id domain namespace. And majority of the data fall into three categories. The first is online gambling. The online gambling is majority in .id abuse, around 57%. And the second is phishing, it's about 40%. And the third is malware, about 2%. This number reflects something we all recognize.

Malicious actor continues to involve under tactic and abuse mitigation must involve as well. That means we need approach that are not only reactive, but also proactive and collaborative. So, we just not suspend, suspend, suspend, but we collaboration with some party.

Next slide. At PANDI, abuse mitigation support.

JOKE BRAEKEN Apologies for interrupting you. Apologies, this is Joke. Could you slow down a little bit?

MOHAMAD SHIDIQ PURNAMA Okay, sure. Next slide. At PANDI, abuse mitigation is supported by two main pillars. The first is policy. We operate under complaint handling framework where report related to harmful or illegal content like fraud, phishing, malware, or gambling. This report is processed and coordinated with relevant authority, when necessary, we need collaboration with other party.

The second pillar is technology and data coordination. To support this project, we develop IDADX. IDADX is Indonesia domain name abuse data exchange. You can visit the IDADX website in idadx.id. And IDADX function is a collaboration platform. So, we can function, the first is collect abuse report.

The third is correlate threat indicator. And the third is enrich investigation evidence. So we not just collect the data, but we correlate threat indicator. And the last is attract cases across the ecosystem. So, after we get the data, we check the other data from other platform or other entity. And this platform helps PANDI to get the better coordination between registry, registrar, and trusted partner. And more importantly, it allows decision based on structure and documented data.

Next slide. For IDADX, we have internal tool, we call BIMA, BIMA is internal detection. In addition, external report, we have also developed a monitoring system. This is my monitoring system. BIMA is a bridge identification and monitoring assistant. BIMA work through internal crawling. So, we crawl all .id domain name, especially a new registered .id domain name, which is conducted by PANDI.

So, every day we crawl the new domain name. This means the system regulates scan, we scan the domain name. And so, after accept, we got the external report. So, we also identify suspicious domain early through internal monitoring. So, before we get report from external, we got the data from internal first. This proactive approach from, we combine with intelligence from some partner like Netcraft, CleanDNS, and TNN. The goal is simple, to improve accuracy, reduce false positive and enable faster mitigation action.

Next slide. And this is abuse handling workflow. Once abuse is detected, we follow a structure workflow. The first is we report our signal is received either from external report or internal detection system. And the second, the case gas truck validation and classification.

If the abuse is confirmed, a notification is sent to registry and registrar. So, we can allow to registry and registrar to perform remediation. If the issue is not resolved on the registry, my process to involve action such as suspension. So, after we inform to registry and registrar, and we not receive a report from registry and

registrar, we suspend the domain name. And once the issue has been corrected and verified, the domain name can be unsuspended.

In certain cases, especially for newly registered domain, containing handful content, and we also implement automated suspend mechanism to accelerate mitigation. For example, if domain name still new under 60 days, and the domain name like a second level, like my.id, this ID or web ID, and the domain name have a content about abuse, we suspend automatically.

Next slide. The current ecosystem challenges. However, even with the mechanism, the ecosystem still faces several challenges. Registry and registrar often receive large volume of abuse notification from different sources with varying level of evidence and credibility. And the sometime brand owner invests significant resources to detect abuse, take down service provider, send much volume of notification, and law enforcement agency may require action across jurisdiction.

The result is that intermediary must review many report manually, which can be inefficient and inconsistent. So, in the problem, still many problems. So, we have a collaboration with my partner is TNN. So, the next step, TNN, maybe from TNN can explain more detail about trust notifier network. Trust Notifier, our concept that my help address to challenge this problem, we collaborate with trust notifier network.

The next slide. The idea is a qualified and trusted entity to submit abuse notification that carry a higher level of credibility. And the scope of collaboration with TNN, but a common DNS Abuse and the business Botnet, malware, phishing, spam, firming, online scam, illegal online gambling, and intellectual property, intellectual property abuse.

And the sometime the framework also define clear execution, such as issues related to freedom of expression or political viewpoint. Trust Notifier must meet certain standard, including expertise, demonstrate, express how to manage the abuse in TNN and operate experience and strong policy in understanding.

And the last. DNS Abuse mitigation work best when detection intelligent and trust mechanism are connected. Platforms like IDADX in PANDI, proactive monitoring systems like BIMA and collaborating with other parties like TNN, CleanDNS and NetCraft and maybe with government can help strengthen to connection. So, because the ultimate, not just single stakeholder, the ultimate is we can collaboration with all partner to solve the abuse DNS.

So, DNS Abuse cannot solve by PANDI itself or maybe not just for registry side or register side. So, the abuse mitigation must collaboration with all party. It looks at collaboration across registry, register and security research like industry partner and ICANN community. Thank you. Thank you very much for attention. Back to ICANN.

BRUCE TONKIN Thank you very much and sorry that you weren't able to be here in person, but you were certainly coming through loud and clear in the room here. Do we have any questions in that presentation? Yes, Byron.

BYRON HOLLAND Thank you for that presentation. Byron Holland from .ca. I'm curious about if you could put or provide a little more context on what you consider DNS Abuse. In particular, your slide referenced a number of times that the domain of main abuse would be, and I think I got the quote, infiltrated with negative content.

And in ICANN's traditional definition of DNS Abuse, that would seem to be slightly outside it. And I'm just wondering how your registry balances sort of traditional ICANN notions of DNS Abuse with what it seems like on first blush when I read it, really content specific. And if I've read it right, then how do you approach that and what would really be considered negative content in that context? Thank you.

MOHAMAD SHIDIQ PURNAMA Okay, thank you. So, negative content, in Indonesia, we must comply with government regulation. In Indonesia, the government regulation like gambling and pornography is not low. So, content including if some domain name or website have the content about gambling and porn, we must suspend the domain name. So, we

just not follow the international rule. So, we must follow the government regulation too.

And we collaboration with government about crawling the data, not just from just internal data. So, we often collaboration with government to check if the domain name suspects gambling or porn. But mostly from registry site from .id, we have already patterned the domain name suspect gambling or porn. So, we can suspend by registry site.

BRUCE TONKIN: Go ahead, Eberhard.

EBERHARD LISSE: Eberhard Lisse from .na. I wonder, are you falling only under Indonesian federal law and regulation or are you also falling under this one federal state where Sharia is the law of the land? I'm not criticizing every 253 ccTLD members, ccTLDs can have their own way of doing things. I'm asking this for interest's sake.

MOHAMAD SHIDIQ PURNAMA: Okay, the number one, we must follow the government rule first. So, after every government rule, we must follow the rule. And the second or the third and the other, we can follow the other rule from, maybe from international rules. So, we must follow the government rule first.

EBERHARD LISSE: That's not what I asked. I asked whether you fall under your federal government. Let me finish. Or also state government, in particular, the one that uses Sharia law.

MOHAMAD SHIDIQ PURNAMA: Oh, Indonesia, not federal or state government. So, we must follow the federal. Maybe we call it federal because we just have the same regulation in Indonesia. We don't have a state maybe like U.S or other country.

BRUCE TONKIN: Okay, any other questions? Yes, him.

KENNY HUANG: Okay, thank you. Kenny Huang on behalf of .TW. Just very similar question because you probably in your local regulation probably mix up with the content abuse versus the dominant DNS Abuse. And in a lot of regulation, probably you have faced very similar situation.

The government difficult to identify what would be the technical abuse, what would be the content abuse. And according to your online gambling, that's specifically mentioned, that was prohibited by law. And my question would be, as an intermediary, do you have general monitoring obligation to fulfill the law or just get a court order or any warrant to suspend the domain name? Thank you.

MOHAMAD SHIDIQ PURNAMA

Okay, currently we have to like IDADX. We have the data from report from public and internal crawling. And then we collaboration with a government too. And we already give the like, and not argument, like how domain name including porn or gambling. So, if we can check the domain name and the domain name suspect gambling or porn, we can suspend by registry.

Because registries in Indonesia, we have a regulation from government and we have a mandate, not mandate, we have like, maybe I call, yeah, we must follow the regulation from government because periodically, every year, the government check the, not compliment, yeah, not like aggression, but how PANDI manage that ID domain name. So, if we not following the rule from the government, maybe we can get the fine from government.

BRUCE TONKIN

Any other questions? Yes, please go ahead, Marina.

MARINA GO AM

Thank you. Thank you for your presentation. I'm Marina from .auDA. Just, this is an interesting area of content. And it's obviously one that, we thinking about our obligation and whether or not we have an obligation.

My question is really around skillset. So, if you're making a decision or a judgment on content, then that requires judgment. So, I'm just wondering whether you have had to specifically upskill people to do this work because somebody's, or is it very clear cut, for

example, pornography, there is a line. So, are you clear, are your people skilled in understanding what constitutes that sort of content?

MOHAMAD SHIDIQ PURNAMA: Yeah, especially for gambling and for porn, we have a team, we call the help desk in internal. So, if we already check the domain name content gambling and content have the porn content, we can suspend the domain name directly. So, this is not gray area because we can see in the content and the website. So, I think this is not gray area, but on a gambling and porn, but except the two categories, maybe we can talk other, maybe other category. So, for gambling and for porn, this is, I think it's not gray area in Indonesia. So, we can see the domain name is gambling or no.

BRUCE TONKIN: Thank you. Any other questions?

CLAUDIA RUIZ: We need to move on, we're over time.

BRUCE TONKIN: Thank you. Nick, yes, please go ahead.

NICK WENBAN-SMITH

Hi and hello, everybody. Good afternoon. Well, you are good morning and a beautiful sunny day in the United Kingdom. Uncharacteristically, I know, it's awful I can say that.

So, just a few minutes here just to talk about the PDP, which Brian gave a good overview on and Bruce alluded to. So, this is a GNSO process and within the ccNSO, I think we all are aware that we are fiercely independent and subject to our own local laws and jurisdiction. And particularly with my chairing of our DNS Abuse standing committee, we are very clear that we do not formulate policy for ccTLDs.

So, what are we doing participating in a gTLD policy process is the sort of challenge. And we did not go into this process lightly. I don't want to emphasize. There was a serious discussion around the ramifications and the sort of the community view that ccTLDs are stepping into this gTLD policy arena. And that is pretty unusual.

Normally we do not. So, I thought it'd be useful just to highlight a couple of points as to why we're doing this. So, firstly, and I think it's always good to step into some of the rooms that otherwise we are not participating in, is to highlight the very low levels of abuse that ccTLDs enjoy generally. It's about a 10th of that seen in gTLDs.

So, it's always good to make those points, particularly because, for example, we have GAC representatives in these rooms and it's always good to emphasize those good points about ccTLDs whenever we possibly can.

Secondly, it's quite a specific scope to this PPP charter. And I mean, to draw an example from my experience, I had a domain name. It came to me in Nominet. It was clearly maliciously registered due to the problematic content on it. But when we looked at the registration records, we saw a mobile phone number in Portugal, a physical address in Italy, name servers in Russia.

And clearly it breached several of our registry policies and therefore is going to be intervened on. However, in that same account with the same registration details, there were another 19 domains. So, of course, we look at all of those 19 for the same sorts of things and ended up spending all of them. This is this exact point for the gTLD policy around associated domain checks.

We didn't wait for a complaint about the other 19. We as the registry could see that they were associated very easily and obviously, and took action on all of them. And that's essentially the objective of this policy.

I think finally, what we see in the gTLD arena can be beneficial and positive for ccTLDs. We're all there to keep our respective communities and internet users safe and free of abuse and criminality and threat actors. So, good developments, and I emphasize good developments. So, we want to get a good policy out of this. Good developments in the gTLD arena can on an opt-in basis be useful for ccTLDs.

So, for example, when we saw the contract amendments that the gTLDs introduced around registrars requiring to take action on

abuse reports, you can see from the DASC survey, a very large number of ccTLDs who obviously, a lot of us use the same registrars as gTLDs. A lot of us opted in to the same sort of contractual language with our registrars in order to create a sort of a uniform approach to those sorts of things for those registrars, which I think is beneficial in terms of raising the standards across the industry and across the different jurisdictions.

So, that's that point. I guess I'll just close on, it came up in the first PDP's presentation. The UK is not exclusively using the .uk ccTLD. A lot of the people in the UK use gTLDs and are targeted by people, particularly large scale phishing attacks. So, for example, my own mother-in-law received a text message about winter fuel payments in the UK, and asked me, hey, is this real? And like, you know, she's elderly and elderly people in the United Kingdom are eligible for a small payment from the government to help out with the extra costs of energy in the winter months.

And it looked very plausible. And we ourselves at Nominet saw 120 of these registrations, but actually we worked out, and this is a joint project we did with the NetBeacon Institute, that we had several thousands across the gTLDs, which were registered in this mass phishing campaign targeting our vulnerable citizens and consumers.

So, I think it is of wider interest to all of us. And ultimately the aim is to reduce abuse and to keep our citizens and consumers safe. So, that is basically where we're at, but I think we want to be

completely transparent about our engagement and our involvement and to sort of be here in front of you, explaining why we're doing this and to answer any questions that any of you might have.

I know Alejandra is there and can speak from sort of council perspective, it was a council decision ultimately, but that's where we are and that's what I really wanted to say about this. Thanks.

BRUCE TONKIN Thanks, Nick. Any questions for Nick on that?

JOKE BRAEKEN Yes, Bruce, there's one question in the Zoom room. A question by David McAuley from Verisign. Nick, did you receive any challenge to suspending the other 19?

NICK WENBAN-SMITH Thank you, David. And thank you for joining. It must be quite an antisocial time of the day for you. And of course, we did not receive any challenge to the other 19 domains. These are domains which are maliciously registered with deliberately deceptive and false data. And of course we received no challenge.

BRUCE TONKIN Eberhard, you had a question.

EBERHARD LISSE

Eberhard; listen, I've got two. I'm one of the appointed members, as you can see there on the left. I'm a full supporter of the ccNSO position and the view that the ccNSO does not have a position and it does not take a view on this. We have just heard from .id where they have got rules and regulations which I could not live under.

We are on the other side of the spectrum in .na where we exclusively work with court orders and we haven't really had one yet. And I need to take a little bit of issue with Chris, which I like to do. We are not really a homogenous group. We have got many more diverse interests than the GNSO. They have got four or six. We have got 253. But ours are not so much diverse and we get consensus all the time and very easily.

We know what consensus is. So, that's why I was a little bit confused by the way they deal with these things. As far as the Working Group is, we basically are at the moment taking, of course, ccNSO Council guidance of basically abstaining from substantive decisions because we are there to provide insight, provide interest, but it's not our problem. It's not my horse in the race.

That said, I agree with Nick. Since many of our registrars are ICANN accredited, they will not run different processes for ICANN registries and ccTLD registries. So, it's good for the ccNSO members or ccTLDs to know what's coming, that they can anticipate it because we don't want the ICANN accredited registrars to have any unnecessary hurdles in their way to leave their money with us.

BRUCE TONKIN Thanks. Eberhard, did you have any comments, Nick?

NICK WENBAN-SMITH No, I think Eberhard, obviously in his very characteristic direct way, I think a lot of us are not for profit, right? We're not, this is not about the money. I think we want to reduce friction with business. We want to make our ccTLDs the most attractive and best sort of choice for our local businesses. Local communities.

I think ultimately this is about doing the right thing. And that is keeping our consumers, particularly vulnerable internet users, safe and free from crime. So, I think that's where I'm coming at this from. And I think that it just seems to be manifestly the right thing for us to do. And we were invited to participate in this PDP and we've answered the call.

There's a lot of good experiences in ccTLDs. We continually emphasize that these are not policies for ccTLDs, that the ccNSO does not have a policy position on these sorts of questions. We're there for information, for best practice sharing, for harmonious and good participation to explain the diversity.

And I think Eberhard was absolutely spot on with that. You can tell that the definitions of abuse within the ccTLD community are extremely diverse from very narrow core order only to all sorts of non-domain name specific, non-technical issues like gambling and pornography. And that is fine. And that is the nature of the

international community and the diversity of the regional jurisdictional and legal positions that each of our respective nation states has.

And we completely respect that. And I think that that's appropriate. But I think, end of the point is that I would like as a result of these sorts of policy initiatives for my elderly mother-in-law to not be receiving lots of phishing emails from gTLDs. And I think if we managed to achieve that, then that will be the test of success.

BRUCE TONKIN

Thanks, Nick. Any other questions? We're going to do a couple of polls. So, we've got on the screen, we had on the screen the Mentimeter poll. Hopefully you captured that. So, our first question that we had is just to get some information on who's in the room. Bit of a control question.

I'm pleased to say that most people in the room are actually related to a ccTLD. But interestingly, we have some people that are both a CC Manager and a gTLD Operator. And so, some of the work that's going on in the GNSO will apply to them.

Okay. I think that's probably got as far as we're going to see. Yeah, next question, which is the more interesting question. This is really just trying to get a sense in the Country Code community, what steps the Country Code Operators are currently doing. So, and this is in the context of the GNSO policy process, that if you are notified

of some form of abuse, do you actually go and check to see if there's abuse on other related domain names?

Interesting, okay. So, you can see basically 50% or nearly half of the room is always actually doing some sort of follow-up. It's a pretty high percentage. And then of that, you can see, of that group, about half of that group only manage their own ccTLD. And we can say maybe 10% of that group are also CC and GNSO Managers, gTLD Managers.

The other high percentage there is sometimes or often. So, if you combine those three together, you're looking at sort of 80% or so are actually doing some sort of investigation. It might not be for every case, but routinely they do look for associated domain names. So, that's encouraging. And also shows there's a lot of experience that the Country Code community can share with the gTLD community in this topic.

Then the next question. We can jump to the next question just in the interest of time. So, this one is really an open question where you can put text in, which is what is your biggest challenge with essentially detecting associated domain names? So, if you're looking for a domain, if you've got a report of abuse and you want to look at another domain name that might have been related to that, what's your challenge in finding the patterns of abuse in your Country Code? What's your biggest challenge, I guess?

False positive has popped up a few times there. So, that's basically a bit saying that the Country Code managers identified a name that

seems to be similar and turns out that it's not. And that following domain is not related to the original form of abuse.

Quite a lot of things coming up there about the challenge is automation. I assume that means essentially that currently they're doing it manually. And it's an expensive process. And so, that a few ccTLD managers are looking to put further automation in there.

Real time, I guess what that challenge is essentially saying, these names will often be created perhaps the day before. And is there an ability to detect these names at the time that they're registered or detect patterns at the time that they're registered so that they never get into the registry or never get into the DNS.

Registrar switching, I think that's what we're seeing is where you'll get a particular party using one registrar to register malicious domains when you've shut it down, which might be that that registrar actually closes the account that's being used to do the malicious registration so they just bounce to another registrar.

Yeah, I think that's probably as far as I can draw conclusions from that information so far. So, perhaps we'll pause there. And then I think the final topic really is, we've got four minutes remaining, but is there any other comment or question anyone would like to make on the work that we're doing on DNS Abuse? But it's partly useful for me as vice chair of the DNS Abuse Working Group, but if there are topics or things that you think as a community we should be working on. Yes, go ahead.

JOKE BRAEKEN Bruce, perhaps we could quickly address the Work Plan for the task. I believe that Nick was going to address this.

BRUCE TONKIN That sounds fantastic. If Nick is prepared to do that, yeah, go ahead, Nick.

NICK WENBAN-SMITH Yeah, thank you for picking me up on that. We had a session on Saturday where we looked at the forward Work Plan and the leadership suggestion, because obviously we suggest rather than dictate, was that having some dedicated sessions previously about AI and financial crime and scams, you can see here the historic sessions that we've had, that we would look at the Seville meeting to have a session with the topic of registry, registrar cooperation, which aligns quite nicely with the PDP work.

We've dipped our toe in the water by talking to the gTLD registries. So, maybe that wasn't so bad. And we will talk to registrars now about how we can work better to combat DNS Abuse and the topic of switching from registrar to registrar, which is something that the registries can see, but registrars individually will just see attack come and go. But we see attacks move from registrar to registrar to registrar as registrars spot them and react.

How can we be better as an industry to cooperate? So, I think that is the suggestion for the next sort of full session of the task of the

Seville ICANN meeting. Happy to answer any questions or be told that's not the right way to go.

BRUCE TONKIN: Any questions on the Work Plan? I think the final question we had is how do you rate this session? So, if you'd like to use your Mentimeter to do that. Not a lot of responses, so four responses, six responses, or at least more people think it's excellent than think it's not great.

So, I think that's a good result. So, I think happy to keep collecting the data there, but thank you for providing that feedback. And we will end the session there. Thank you, all.

[END OF TRANSCRIPTION]