ICANN84 | AGM – ccNSO: DNS Abuse Standing Committee
Saturday, October 25, 2025 – 10:30 to 12:00 IST

CLAUDIA RUIZ

Hello, and welcome to the ccNSO Domain Abuse Standing Committee session. My name is Claudia Ruiz, and I, along with Joke Braeken, are the participation managers for this session. Please note that this session is being recorded and is governed by the ICANN Community Participant Code of Conduct, the ICANN Expected Standards of Behavior, and the ICANN Community Anti-Harassment Policy.

Please observe the following guidelines to participate in this session. If you would like to speak during this session, please raise your hand in Zoom. When called upon, virtual participants will unmute their microphone in Zoom, onsite participants will use a physical microphone to speak and should leave their zoom microphone disconnected.

For the benefit of other participants, please state your name for the record and speak at a reasonable pace. Thank you. And with that, I will now hand the floor over to Nick Wenban-Smith, Chair of the DASC. Thank you.

NICK WENBAN-SMITH

Gracias, Claudia. Good morning, everybody. Welcome to Dublin. Welcome to this in-person session of the ccNSO DNS Abuse

Standing Committee. My name's Nick Wenban-Smith from UK Nominet, here with my vice chair, Bruce, from .au. So, as usual with our in-person meetings, we are taking a-- Okay, thank you very much. The speak slowly thing as I think specifically put in for my benefit. So, you can see here the agenda for today's meeting. We have 90 minutes. So, it's quite a busy session for the DASC at this ICANN meeting, and we can talk through what's coming up.

But apart from some minor administrative matters, the main thing I want to focus on is the upcoming flow of work going forwards. So, just start to put your thinking caps on about what are the pressing topics that we want to talk about in the next 6 to 12 months as we go through the next series of ICANN meetings, and start to think about what would look good in terms of focusing on an agenda setting program.

The other thing I did want to just highlight is that we have had some quite successful intercession sessions in terms of community webinars in between the actual ICANN meetings. And I think that's quite a nice way, particularly as we look to quite a big gap between the next in-person ICANN meeting in Mumbai. There are some, yeah, community updates and intercession work that is quite usefully done just so that people stay in touch with the work of the DASC and start to think about, you know, the topics of DNS abuse and what more measures and things people can do in the community.

So if we move on to the next slide. So I did just to focus on the agenda there, and I should ask, are there any items of any other business that I need to factor in, in terms of trying to keep this meeting according to some sort of organized timetable and schedule? If there's any other items of business that people want to discuss, then feel free to either raise their hand in the Zoom or let me know, and I will try to make sure that there's time to have that discussion.

Fine, thank you. So just a little bit of a recap about the DASC. So, because this is the ccNSO, I feel I'm repeating myself, but I know there's many of my friends from the GNSO community here. The ccNSO does not formulate policy for ccTLDs in this area. This is not a policy making body in that context in the same way that the GNSO would be. But it is much more of a best practice sharing insights, information, sort of show not tell type of environment that we try to have in a very positive and constructive way. It's a very serious issue, but every ccTLD has its own respective laws, jurisdictions, communities practices.

So it's much more of a sort of discursive sort of capacity building exercise. And although we're not here to create policy, I don't think any of us should be under any illusion. Ultimately, we want to drive down DNS abuse, so, that is something that we're measuring and something that we actually actively seek to achieve, but it's not through policy development as such. Okay, next slide.

So, as you can see, we have an abuse library, there is the dedicated email list. Slightly concerning is the next year is 2026, so that means that we are going to have to repeat the global survey of ccTLDs. So, every two years we do a global survey of ccTLDs, how they're experiencing DNS abuse. Very interesting to see the differences between 2022 and 2024.

Much more awareness, much better obtaining of metrics, use of AI, a lot more sophistication, so that's quite an interesting thing. So, that will be repeated. So, there is a survey team, which will be spun up next year to dust off the questions to look at the feedback from the last survey and then to repeat that survey. So, that'll be coming up in 2026.

Useful sessions that we've had, they are obviously all in the recordings and archives, but we've had deep dives on tools and measurements for ccTLDs to look at them, the levels of abuse that they have in their own ccTLD backyard. We had a specific look with friends from the Registries Stakeholder Group in the gTLDs for the contracts, which they have in the ICANN standard agreements around DNS abuse mitigation and obligations on registrars to act promptly when they receive credible and actionable abuse reports.

And yeah, we've had a look at the role of registration data and accuracy in combating DNS abuse. And most recently we've had specific deep dive into the serious issue of online scams and financial crime and the intersection with domain name registration in particular and the ccTLDs.

Next slide. So, when we looked at this question previously two ICANN meetings ago, I want to make it clear that this is not the democracy of Rome, but we do listen to our stakeholder feedback in terms of setting the agenda. So, we take our community very seriously and we try to listen to what people are interested and want, and then try to deliver that in terms of helpful and interesting content.

So, as you can see here, we asked the question around, well, what are the topics that we should be addressing going forwards? And AI came out number one, so, you'll see in the rest of this meeting that there's a strong focus on artificial intelligence. So, for example, on Monday, Tech Day, we have presentations from I think three or four ccTLDs around the use of AI and mitigation and detection of DNS abuse in those ccTLDs and discussion of that.

Fraud and financial crime came second. So, in the last couple of meetings, we've had quite a little look at that topic. And then, lower down the list, we've got things like partnering with the registrars, obviously, the partnership between a registry and a registrar as part of the ecosystem, and maybe leveraging those relationships more effectively so that we work in cooperation and coordination with our registrars, those of us who have registrars, not every ccTLD operates for the registrars.

Looking at compliance, obviously, if you have contract terms to require abuse mitigation, then they mean nothing without contractual compliance. So, that came up as a topic. Specific deep

dives on phishing. Phishing is the number one problem in terms of domain name registration and DNS abuse. Child sexual abuse material, governance models, cryptocurrency, and gambling was the results of last times informal polling.

And I say it wasn't a democracy, and I must speak more slowly. We did exactly follow the priority, which was set by our community results. So, any thoughts or questions or comments on the proceedings so far? Stunned silence. What do you think, David? You are looking at me quizzically. I can tell you're thinking something, although you don't--

DAVID MCAULEY

Thank you. Thanks, Nick. It's David McAuley speaking for the record, member of Verisign and a member of the DASC. No, I think your summary is great. I will mention that the work on the DNS abuse library and on the email list, as we get into discussions for work plan, I think we'll revisit that, tweak it, and look at how at the incidents of usage value, all of those kinds of things. And so maybe I'm anticipating a discussion to come on our work plan, but I thought your summary was great. Thanks.

NICK WENBAN-SMITH

Thank you, David. Any other thoughts? Bruce, how are you? No other thoughts. Okay, good. Do people value the work? Oh, come on.

ABDALMONEM GALILA

Yeah, this is Abdalmonem Galila for the record. Actually, what you said if I recall well, that at Tech days there will be DNS abuse sessions that will consider ccTLDs-- consider active mitigation or using AI for mitigation of DNA abuse. My question is here, are there any AIs that could be used by other ccTLDs in order to [00:11:52 - inaudible] active mitigation for DNS abuse? Thank you.

NICK WENBAN-SMITH

So, it is a great question. Thank you for the question. And I think there isn't, and that's what we want to achieve. So, as part of the tech day activities on Monday, we have, is it an hour or an hour and a quarter of, one hour, where we are having presentations from ccTLDs.

So, we've had a community call for presentations on the topic of AI, and we have some volunteers ccTLDs who are gonna come and present to the ccTLD community examples of real-life use of AI in their ccTLD for the purposes of detection and mitigation of DNS abuse. It's for that exact reason to try to create understanding this is what we tried, this is what works well, this is what we tried, didn't work so well to build a higher standard across the globe in terms of the use of these new AI tools to help to combat DNS abuse.

Yeah, so, we are working on that. And interestingly, on Wednesday morning, I think the ccNSO is having a meeting with the GAC, the Government Advisory Committee, and they specifically want to hear from us around the use of AI and ccTLDs. So, that is another high interest topic with us and also the governments. So, yeah, you

can see it was the number one issue in terms of prioritization that we received two meetings ago, and that's what we're delivering, I hope this meeting. Bruce.

BRUCE TONKIN

Yeah, just to elaborate further because we have heard that request also from members of the GAC that are saying there's some software off the shelf they can use. I think the reality is a number of ccTLDs are exploring the use of AI and effectively building in-house solutions, but it's not like there's something off the shelf that you can say, here, go to this website and download the AI magic. It's something that we're each working on.

NICK WENBAN-SMITH

And I think looking forward to the survey for 2026, it'll be really interesting to see the increase in adoption of AI in different places, in different techniques, in different strategies to leverage AI technology for this purpose. In 2022, AI wasn't a topic. 2024, about a third of the ccTLDs are using AI in some way.

And I think it'll be super interesting in 2026 as we try to socialize and promote good AI practices to see whether it goes to maybe more than 50% of ccTLDs starting to adopt AI now. It's been a dramatic change. It's been the most significant change, I think in the landscape over the last four years. Oh, Pablo.

PABLO RODRIGUEZ: This is Pablo Rodriguez for the record. Thank you, Nick, for a great summary of what you were explaining. And I would like to contribute to the conversation regarding AI tools.

While it is true that some ccTLDs are looking for ways of developing tools, AI tools in-house, it would be interesting also to identify which AI tools are using backend providers for those ccTLDs that they manage that perhaps could give us also another side of the spectrum that could help us out identify what those tools are and what works for them, what doesn't work for them.

I know that it might be some obstacles with intellectual property and so on and so forth, but whatever they can contribute to this conversation perhaps would be helpful. Thank you.

NICK WENBAN-SMITH: I think that's it's a great topic and I need to be a bit careful, but when you have a service provider, you are the boss, you're the customer, so you should be ahead of the curve and say, Hey, the community is developing these sorts of tools. You our supplier should be exploiting them to the full to maximize the benefits, and we want that as the privileged customers, right? So, I mean obviously, we know there are plenty of the suppliers, and some of them are in this room, I'm sure.

But yeah, I think I'd like to see a collective rising across the whole supply chain, whether you are the registry manager yourself or you are the supplier for fulfillment of registry services so that we create

common standards and higher practices and push down their levels of abuse less according to our charter.

PABLO RODRIGUEZ: Indeed, I think it would be a great dialogue to say, are you protecting us? You're my provider, are you protecting me with some kind of AI tool in addition too? And if you're not, would you consider doing so with some other tool? So, that would be a great dialogue.

NICK WENBAN-SMITH: Okay. Thank you. Good point. Bart, sorry, what have we done?

BART BOSWINKEL: Not, you haven't done anything. People, there are chairs at the hat table, so you don't have to stand in the back. Probably they don't allow it. So, if you could take one of the empty seats at the hat table, there are five people standing in the back. So, there are plenty of chairs in there.

NICK WENBAN-SMITH: And okay, is there a question in the Zoom room? Sorry, I'm useless at following that and speaking at the same time.

JOKE BRAEKEN: There's indeed a question in the Zoom room. Shall I read it out loud?

NICK WENBAN-SMITH Please, do.

JOKE BRAEKEN Does DASC use the same definition of DNS abuse as I can? If not, can I get a link to the definition used?

NICK WENBAN-SMITH I think Dr. Tonkin is best placed to answer that question.

BRUCE TONKIN Yeah, I just posted something in the chat, Joke. When we use the term DNS abuse, if you like, there's a contractual definition that we do use that relates to what's in the gTLD community as well. But when we've done our surveys, we've asked ccTLDs what other forms of abuse do they manage? And that varies.

So, some ccTLDs for example, look at fake shops, other ccTLDs might look at gambling, there's obviously child material, most ccTLDs will take action against that. So, I think as a community, we go beyond just phishing and malware, but it varies. But when we use the term DNS abuse, we're referring to the ICANN definition if you like. But this group does look things a bit broader.

NICK WENBAN-SMITH That's exactly right. So, we had sort of existential question about DNS abuse and definitional terms when we set up our charter,

which I remember well. And don't get me wrong, as a lawyer, I'm very keen on definitions and clarity and that kind of thing. However, I've seen a lot of time and a lot of heat and light in the community discussing the definition of DNS abuse and not actually doing anything about it.

So, I think it was kind of like, we don't want to re-litigate things which have already been discussed in other forums. So, we will generally follow the ICANN definitions. However, because we're ccTLDs, we each have our own custom law jurisdiction, and so, necessarily it is different in different places. It's not like there's a ccTLD definition and a gTLD definition. Like each ccTLD will have a slightly different perspective, and quite often, because we're not constrained by the GNSO ICANN bylaws, we are not sort of either helped or hindered, depending which way you want to look at, it by the sort of the content issue.

So, for example, in the United Kingdom, we have specific legislation requiring the ccTLD to take action on child sexual abuse content. That's a content issue. You could have fluffykittens.uk, it has nothing to do with the text of the domain name. It's not a phishing or anything like that, it's not a technical abuse, but the content is highly illegal and problematic, and we are legally required to take action on it. That's just a United Kingdom specific thing. Every country has similar sorts of things and they are different.

So there's not a super useful waste of time to go through this sort of definitional type things, but I appreciate from a sort of academic

doctrinal point of view, a very interesting point for discussion and just throwing it out there. Was there anything else on the Zoom? Thank you. Fine. So, this is the interactive part. You're very lucky I haven't had anybody standing up and sort of doing exercises and things, so, all you have to do is to pick up a phone and do the Mentee thing. Look, I'll even do it myself.

Better work. So, we're all set. I'm waiting for the presenter. Oh, that's me. So, I just want to have a little bit of a temperature check in the room as kind of like who we are. But we have gTLDs.

BRUCE TONKIN Yeah, but you're not doing it as a ccTLD.

NICK WENBAN-SMITH We sort of are, it's like geo. Anyway. So, mostly ccNSO. 1, 2 3. How many is that? Who's good at numbers? 30, 40. There's more than 40 people here. Anyway. Fine. Thank you. I'll just put that question here because sometimes we get a quite an even amount of ccTLD people and non ccTLD people.

And when we are coming through to the priority setting and agenda setting, we are obviously a ccNSO group, but actually we're quite a broad group and part of our remit in the terms of reference is to reach out to other communities. So, it's very welcome to have other people here, but primarily we're here for ccTLDs. Fine. So, next question then. Sorry, can somebody who put other, what else is there? I guess government. When do you put, Brian?

BRIAN BECKHAM Well, I would put other.

NICK WENBAN-SMITH Okay. And what's your official affiliation?

BRIAN BECKHAM So, I'm with WIPO, the World Intellectual Property Organization, and so we manage the UDRP, which is applicable in gTLDs, but then a lot of ccTLDs have either adopted it or adopted variations, but officially an ICANN word observer to the GAC.

NICK WENBAN-SMITH Thank you. Okay, all right. I just wondered whether we should, just for future reference, whether we should have tried to put GAC or ALAC and things in terms of other-- because other's quite a big category. It's the second biggest category and it's not particularly club. Anybody else in the other category want to talk about their affiliation and interest? Chris.

CHRIS LEWIS-EVANS Thanks, Nick. Chris Lewis-Evans for the record. We're a provider of DNS abuse services that use AI. So, obviously, very interested in this. And to the previous point, we'd be really interested to share what we can such as like evidence and standards that supports higher accuracy of AI tools. So, not necessarily to do with us, but

what we learn around that, that we can, we'd love to share. Thank you.

NICK WENBAN-SMITH: Thanks, Chris, and well done for getting in the sales plug. Okay. So, next question. Okay. So, this is a repeat of the survey questions that we did in ICANN82. So, for ccTLDs, so only answer this question if you're in a ccTLD or ccTLD affiliation, what do you think we should prioritize given that we've had AI and got that? So, I don't want to have AI again, we have to put AI again.

So, it's sort of magnetic, isn't it, watching us? So, AI and scams were the last two favorite topics which we've already tried to address. Is that a feeling that we haven't sufficiently addressed those topics and they're still the number one thing and we should do more of the same before going down to the lower priority stuff on, say, cooperation with registrars or workshops on phishing?

Is there any person willing to commentate that? So, we're gonna repeat this in a second, but for the people who aren't ccTLDs, the idea is to see whether the ccTLDs vision of priorities and interest topics is the same, or if there's a difference between non ccTLDs interests and topics and priorities.

BRUCE TONKIN: I think the comment I would make is AI is used to feel like on both sides of the ledger. So, I think phishing is actually getting better through the use of AI. The phishing emails, it used to be that you'd

advise people and you'd say, if you see something with lots of grammatical errors, it's probably not from your bank. Now, if you see something with perfect grammar, it's probably not from your bank.

So, the quality of the phishing attacks if you like, is getting higher. So, I think that's why there's probably interest in both really. It's like how's AI making DNS abuse, if you like, more prevalent or stronger, and also what are we doing to counter that?

NICK WENBAN-SMITH: It's the sort of perpetual arms race in terms of the, the bad guys. They're not stupid and they've got the same tools. Great. So, we will still-- when it's moving like that, is that because more people are still putting in, people had enough time to do that, is it? If it's sort of settled, then we can--

BRUCE TONKIN: I'm not sure what bad regs means. Oh, not bad registrations, bad.

NICK WENBAN-SMITH: Yeah, I think so, yeah.

BRUCE TONKIN: As opposed to bad regulations.

NICK WENBAN-SMITH Well, there's no monopoly on bad regulation, is there? Cool. So, no spoilers, but we're gonna repeat that exercise, but for people who are not ccTLDs and see what they said. Can we move to the next thingy? So, this is for everybody else in terms of what should be-- Sharing? Oh no, please don't. By the way--

BRUCE TONKIN This is from anybody.

NICK WENBAN-SMITH So, somebody's doubled down on the sharing of zone files. Is that you, Brian? So, just because there's a bit of history to this, if you're a gTLD, ICANN requires you to provide a copy of a zone file and that is available for free to anybody who is interested under quite a light touch license. And ccTLDs generally don't. Do you publish your zone file?

So, in .uk, it was kind of like the zone files sort of sacred, and then we decided that actually we would let people use it, and it's kind of fine just for other ccTLDs who are interested in that. But what's interesting here is it's completely different, right? Well, is it completely different, sort of different?

Fraud prevention. This is quite interesting because a lot of this stuff is not actually technical abuse in the ICANN definition, but you are the sort of non ccTLD ICANN community. Yeah, I mean the word cloud, and we found that before actually in the prioritization where you have, say, some people say scams and some people say

phishing. Well, there's quite a-- if you look at the Venn diagram of scams and phishing, there's gonna be quite a big overlap between the two things.

So, you can kind of group them together in terms of topic. So, one of the things that is going on, and I wanted to talk about this, I did actually think about doing a slide on it, but I kind of ran out of road in the preparation phase. The GNSO has put out a public comment on a couple of PDPs around abuse, which have been initially suggested through NetBeacon.

They did a white paper and they came up with some low hanging fruit in policy topics for gTLDs. Firstly, that if you're a registrar and you allow ungated access to resellers and third parties to API for bulk registration, then that's kind of a-- in housekeeping terms, that's sort of walking out of your front door and leaving it wide open for crooks. So, maybe we shouldn't do that so much.

And secondly around if you have a verified abuse report in an account for one domain and there are a hundred domains in that account, then maybe take a look at the other 99 in that account without waiting for an abuse report for them on the basis that one is likely to be highly indicative of abuse in the same account. So, associated domain check as I think it's called.

And I did actually put in a comment saying this is a good idea in the public comment period, but if there's anything that ccTLDs can do to try to encourage adoption of best practices across other parts of the community, then I think that's something I'm quite interested

to lend our support across that because I've said it frequently, a ccTLD and a gTLD, we're still TLDs, we're still exploited by the same threat actors, and if we can raise standards so there's not gaps between our policies and practices and create opportunities for those threat actors to exploit vulnerabilities or policy or operational gaps, then we should try to help in that regard. Super interesting.

So, financial scams came up again, scams, broad. Obviously, that's a sort of a wider thing than just the sort of DNS technical abuse in terms of phishing and malware, right? ccTLD blockbuster. Can somebody cast a bit of-- Welcome. Yeah. Step forward, it's very friendly and inclusive, so thank you. And state your name and affiliation please.

VIVEK GOYAL

Sure. Hi, my name is Vivek Goyal. I run a company called LdotR, and I'm also a member of the GNSO Council, but these comments are mine. Many ccTLDs are also run as gTLDs, .ai, and so many of them, and many ccTLDs do take very proactive actions when complaints are gone to them.

They block domains, they shut down those registrants, but the data only stays with them. If ccTLDs together share this information with each other, it can help a lot of abuse being taken down and prevent these guys from jumping from one TLD to other TLDs and others. Now, I know every country has its own regulations and

sharing, but if somebody starts that, others will see the value and join in that effort. Thank you.

NICK WENBAN-SMITH: So, I know that there's a like a TLD hopping list, where if the same string is, say with CSAM, that's the most common use case, there's particular strings and it's like, well, you shut it down in one TLD and it just goes to a different TLD, the exact same string, right? So, maybe share a bit more information about that. I think it's an interesting suggestion, and I think it has some utility.

One of the issues that we have in the ccTLD world is the linguistic diversity because something which is problematic in Hindi or whatever is meaningless in English or French or trying to think of another one, Spanish, and some words in Spanish, I wish I know, have a completely different innocent meaning in English. So, it's a technically complicated thing, but there are maybe risk areas, but we can talk about this. Yeah, feel free. Yeah, carry on.

VIVEK GOYAL: In my mind what I'm proposing is this is information. As a ccTLD, you receive this information, then you decide which ones you want to act on and not just blindly turn off everything. But as of today, the information sharing is not there. Let's start with information sharing and see how much impact this makes. If there's something related to CSAM in the domain name abuse, in either language, you will take action against it.

NICK WENBAN-SMITH Completely agree. And I suppose what you're talking about is trying to socialize higher risk strings, right? Alan, did you have your hand up?

ALAN WOODS Alan Woods from CleanDNS for the record. An awful lot of the themes that come up here as well about data sharing. Like obviously data is vitally important, but what we're finding, especially with the advent of AI as well, is that there's an awful lot of data. And some people will contest that signal is signal, but you must remember signal is also noise.

So, the more data you have, the more expensive it is to find the actual point of that data. It takes a lot of time, it takes a lot of effort, and AI can help with that, but it needs to be in a way that we maintain things like due process, human rights, there's gonna be a lot of deep human rights impact assessment conversations throughout this week as well.

So, maintaining good data in a sea of noise is something that we need to be focused on. And as you're looking at policy development, or not policy, but discussing this, keep that in mind to the forefront as well.

NICK WENBAN-SMITH No, I think that's a good point. Are there any other thoughts or observations in terms of the discussion and prioritization? I think

one of the early comments was taking action, and I think it's good to have a good discussion about something, but it's nice to-- In the IGF world, one of my amusing phrases is concrete outcomes, which usually means the literal diametric opposite of a concrete outcome.

But I would actually like to see something useful in terms of community practices or information and things come out of these sorts of exercises. Because the biggest most valuable resource we have is our time and effort and input, and I would like to see us doing things which move the needle in terms of combating abuse or raising standards across the ecosystem. Any other thoughts? Anyone? Brian.

BRIAN BECKHAM

Yeah. Thanks, Nick. Brian Beckham. I think when you look at these word clouds, either this one or the previous one, obviously, a lot of themes kind of emerged to the top. So, I wonder, this is a, I think a theme that's been explored in several Ike meetings over several years. So, it leaves me wondering what are the obstacles to kind of turning the corner on taking action? I think this was kind of maybe the point you're getting to.

So, if it's about sharing information or tools or best practices, then, what's getting in the way of that happening? Is it something that there should be a working group or informal gathering of ccNSO or ICANN or other interested people, but what can kind of be a

moment to take action and start to leverage some of these things that are on the screen?

NICK WENBAN-SMITH: What I think is interesting is that, say fraud prevention and financial scams, if you put all those ones together, then that would be like a-- because they naturally group, and so that would be the biggest thing. That is not actually a DNS abuse per the ICANN definition. So, actually, the non ccTLD ICANN community is telling us to take action on stuff which isn't technically a technical abuse per the ICANN definition.

Have I read that correctly? Because that's kind of interesting thing from my perspective. And I think I got a good laugh when I said we shouldn't be the DASC because it's not DNS abuse, It's just abuse. We should just be the ASC. And that seems to be what-- have I read that wrong or tell me? Pablo.

PABLO RODRIGUEZ: This is Pablo Rodriguez for the record. One of the things that the community may be saying, especially with the area of fraud prevention, has to do with whatever it is that we're doing to avoid abuse, is going to result into a prevention of fraud.

And so, becoming aware of what are those things that we can do within the DNS and what are those things that we can do within the interaction among other groups, ccNSO, GNSO, GAC, and others, the end result will be that fraud prevention. So, it may not align

exactly with the definitions that we may have, but without a doubt, it's going to arrive to the same destination. That's my perception.

NICK WENBAN-SMITH

No, thank you. Sort of slight digression, so, my birthday's on Halloween, so my wife said, oh, what would you want for your birthday? So I said like, world peace. And it'd be like fraud prevention. There's a fraud prevention, presumably in the context of domain name registration and the DNS. We can't wave a wand and stop fraud tomorrow because fraud has all sorts of things, there's all sorts of vectors into fraud, whether that's there know people phoning me and off, I've got some great job opportunity with TikTok.

Again, so, there's nuisance calls, there's text messages, there's other ways to get into it other than the DNS, right? And sometimes there's a domain name involved and sometimes there's not. So, in terms of the domain name system and fraud prevention, what more could we do? Is that the same as phishing essentially, or is that distinctive? Peter, do you want to comment?

PETER KOCH

Okay, this is Peter Koch, DENIC. Good morning. First of all, I'd say I don't agree that there is an ICANN definition of that word. There's a gTLD definition of that word, but [00:42:48 - inaudible] should be destroyed. I believe it could be a bit of an overreach to read into

this that people are suggesting if ICANN is not extending its mandate, then the ccTLD should.

I'd focus on the prevention part which suggests to be proactive at some point instead of being reactive, so let's not talk so much about take downs and everything. But if we have a connection, and I think that is agreeable in a way between fraudulent data being presented at registration time or other indications of somebody's trying to hide their identity, that's the one.

And fraud is a much nicer word there because it's more to the point, I believe, than abuse or DNS abuse or something. And of course, I didn't write that, so I'm not just applauding to my own thing, which I didn't actually, but it makes sense. I don't think it's a big deviation, maybe a refocusing of the efforts. Thank you.

NICK WENBAN-SMITH No, thanks. And I think it's an interesting point because fraud is essentially dishonesty and deception, and that is a broader topic than just the domain name registration. And one thing we haven't talked about, and I don't know if it's the same for you guys in the EU, which is a large mature TLD, but a lot, maybe even slightly, the majority of the domain name abuse problems is actually nothing to do with a domain name, which is created to cause abuse, but actually is an innocent domain name may be quite old with not very good security and patching, which is compromised, and that is used as a vector for abuse.

So, is that something that if we're talking about fraud prevention in the sort of more holistic sense, so should ccTLDs be more proactive about trying to get up-to-date software and security patching so that compromise a website doesn't happen, how do you get in touch with the website owner? Would you do something in terms of compliance if the website owner doesn't put their house into order after an escalated intervention?

There's all sorts of interesting areas which could be explored, not just the-- because I think there's quite a high understanding of the problem of abusive registrations and phishing campaigns and sort of you see them happening, you suspend them quickly and you kind of move on. This says to me that we should be looking at things in a more holistic way, if that makes sense. Is that fair?

PETER KOCH This is Peter, for the record. You may well say this, but I think the suggestion also allows the opposite interpretation. Like you strengthened the focus by widening it, where my reading of this was narrowing the focus. It's a bit where you say you amend something and then remove it.

NICK WENBAN-SMITH It's interesting.

PETER KOCH Penalties of the language, but I won't win this race with you, sorry.

NICK WENBAN-SMITH: You may well win the race with me. I am self-aware enough to know that I have my own sort of biases and prejudices when it comes to these sorts of topics. That's not too philosophical. Okay.

CLAUDIA RUIZ: We have a hand up.

NICK WENBAN-SMITH: Oh, great. And is that in the Zoom or is that in the room or both? Rowena. Welcome.

ROWENA SCHOO: Thank you, Nick. It's Rowena Schoo from the NetBeacon Institute. I just wanted to add something to the discussion of fraud prevention and how that intersects with I guess the concept of DNS abuse. And I'm gonna put something in the chat as well. We've written a blog about how we think tackling fraud at the point of registration, using tools from payment providers could then go on to help prevent malicious registrations that may then turn into DNS abuse further down the line, be used for phishing and things like that.

It's probably more relevant to retail registrars, but I think the link to ccTLDs is either whether you take direct registrations as a ccTLD or it comes down to how you're managing your registrar channel and having conversations about which registrars have large

amounts of malicious registrations, and are they doing everything they can to kind of prevent fraud at that point of registration. It's just another angle of thinking about the topic and the connection between fraud prevention.

NICK WENBAN-SMITH: Oh, thank you. And I think you weren't here at the time, but I asked earlier about whether ccTLDs should be agnostic or try to help in terms of the PDP stuff for the thing. And I know that was partly your genesis. I wondered if it was unfair if I put you on the spot about that is should we just watch with our popcorn or should we get in and put our mud guards on?

ROWENA SCHOO: I think being generally interested, aware, and supportive is a good place for ccTLDs to be because there are parallels between what happens in the gTLD space and the CC space. I think there's things you can learn from what happens in the gTLD policy that you might want to implement even though you're not bound from it. And there might be ways you can contribute to those conversations as well.

NICK WENBAN-SMITH: No, thank you. And it's actually a sign of democracy because I actually always put in, when it comes to my personal prioritization, I put like partnering with registrars because the same registrars, predominantly the large registrars are also gTLD registrars. S, if the

ccTLD policies can combine and create sort of standards, really make it easy for the gTLDs to do things at scale uniformly and properly and reduce abuse across all of the ecosystem.

As you know, of the top 10 TLDs in the world, seven of them are ccTLDs in terms of the biggest registries and volume of domain names. So, I think that people are missing a trick if they don't include the ccTLDs in that, and if we can have a great relationship with registrars to push down abuse across everything, whether it's a ccTLD and a gTLD and the standards are common, then I think that would be like a beneficial outcome.

ROWENA SCHOO

Yeah, and I think if you are looking at raising expectations for registrars or looking at changing your policies, if you're doing that in a way that's already consistent with something that they have to do in a gTLD space or have contributed to, I think that's gonna make them their lives easier rather than making new and different policies. Although I do recognize that every CC is different and has a unique local circumstance.

And just finally, I don't think it's necessarily reflected here, but I thought your points about issues of compromise were quite interesting. because certainly what we see in our data is that it's more often the case that ccTLDs, particularly older, larger ones, have a larger proportion of abuse that is related to compromise,

and I think that's gonna be a particular challenge for that could be appropriate for CCs to sort of think about.

NICK WENBAN-SMITH: No, thank you. It is sort of something that I've been thinking about a lot because, obviously, as you know, in the UK we have more abuse through compromised domains than we have from malicious registration. So, you can push down the amount of malicious registrations, but actually that is focusing on an area which isn't actually the majority of the abuse.

So, kind of beneficial, but you are missing, what is it, you're not seeing the whole of the moon, if we say, in that context. By the way, it's kind of the law in these meetings that you have to interact and say something interesting. So, if you haven't volunteered anything so far, I will randomly pick on people, and there's plenty of time left in the meeting.

ROWENA SCHOO: You have hands in the Zoom room?

NICK WENBAN-SMITH: Oh, I have hands. Okay, great. Thank goodness. Alan. But he's actually here. Okay.

ALAN WOODS: Thank you. Alan Woods for the record. I was trying to play by the rules and put my hand up in the room as well. So, just something

that Rowena said there kind of reminded me of something that's very different obviously between the ccNSO and the GNSO especially in the context of having lived through many years of the DNS abuse conversation at the G level.

And that is, it's a question of politics as well, and that is, when DNS abuse is talked about in the GNSO, it's about minimum expectations, it's about contractual obligations, it's about making sure that they must do something, whereas you're freer to have a conversation that could extend beyond that minimum expectation about the good, the better, and the best practice as opposed to being limited by, as soon as you have a conversation about, it gets into a contract.

So, I think when you're talking about do you want to drop the D, it's very possible that that is something that you're more free to have that conversation without it ending up in a contract. But again, balancing that again, is what happens here will then reflect in the conversations within the GNSO as well. So, there is a balance, but I think you're freer to have those conversations.

NICK WENBAN-SMITH No, thank you. And actually, I was just thinking that yes, it's all very well to align with the gTLD policies provided they're any good, and they might not be, or they might not be good enough for what our aspirations are to have no abuse, and no abuse, whether it's DNS abuse or fraud.

And I think reflecting, I don't know, Brian sits more in the GAC space than I do, but I think the GAC are much more interested in fraud prevention than the technicalities of is it DNS abuse through the doctrinal black and white of the definitions like, well, fraud's fraud and we know when we see it and you guys should do more if it's in your wheelhouse. Rowena.

ROWENA SCHOO Just on the raising the standard beyond the floor, I think I've said to the ccNSO before that incentive schemes are also a really interesting thing to look at here in terms of how you can potentially work with your registrars to incentivize them to go above and beyond and give them benefits for achieving well beyond the floor. Like try to create a ceiling or something for them to aim for.

CLAUDIA RUIZ We still have a hand.

NICK WENBAN-SMITH Another hand. Okay, great. Sorry. Thank you, Claudia.

DAVID MCAULEY Thank you. David McAuley speaking. Nick, I was just gonna ask you a question about the time. I have a comment, but it's procedurally about the inner workings of the DASC, and so it should probably go

near the end. And I was curious on time, how much do we have? Are we getting near the end?

NICK WENBAN-SMITH I think we've got another half an hour. We're going through to 12, right?

DAVID MCAULEY Okay. I think I'll comment later then.

NICK WENBAN-SMITH No, you have to comment now.

DAVID MCAULEY Well, I can comment now and keep it brief. We're getting the value of all these very good observations from outside the DASC, but in the DASC, I would suggest that before ICANN85, we may want to look at, consider at least, reconstituting ourself. And let me just go back a little bit and talk about the two committees we have. We have one subcommittee that you and Bruce lead that is on surveys.

It's an excellent subcommittee and it's produced a lot of great information and will do so in the future. But the subcommittee that I have led, which has created the DNS abuse library and the mailing list, we have had a small group, six of us, we've done really good work, but I think we need to look at are we getting actual use to the products that we've created?

And I think we might want to consider trying to merge the list and merge the library in the following way. Taking advantage of all these kind of comments, should we not consider a list that's not something that people come to look at, but rather something that we as a DASC push out information once a month, maybe. This is a lot of work I'm talking about.

But to merge the list and what we call the library, but an available pool of information, sort of assess it in our working meetings to pick the top three or four and push those out every month and try and engender a conversation that way and share this information. And the reason I mentioned it is, I wonder how much use our library is getting. It's an excellent library, but it is a place that people have to go, and I'm just thinking in our working meetings, I think we should take a look at this and think about an alternative.

Not making a judgment, I'm just saying we've been going along in good time, it's probably a good time to take a look. So, that internal comment, I hope does not derail these excellent observations we're getting from folks about substantive things we might be looking at. Thank you.

NICK WENBAN-SMITH No, thanks for that. My mind has been going along that path as well. As you know, I'm a firm believer in the doctrine that the definition of insanity is to repeat doing something and expect the outcome to be different. If it's not working, then we look at something else and we're masters of our own destiny and we

should be thoughtful about how we devote our time and resources. I also know that things have changed a lot in the last four years.

There's a huge amount of resource and a lot of frankly, competition for eyeballs on abuse related topics. So, if we've fallen down the list, then either we stop doing it or we do it in a different way, I'm completely in agreement with that personally. But I think it's a discussion for the wider group. Is there any more hands in the thing? Okay, great. Sorry. Every time I chair these meetings, I say I'm gonna keep an eye on the Zoom and then I never do. Fine. So, any more for any more? Brian.

BRIAN BECKHAM

Yeah. Brian Beckham. I think David's idea is a really good one. It's being more proactive and maybe even liaising with organizations like Center and LACTLD and so on to sort of more proactively share information and best practices could be useful.

NICK WENBAN-SMITH

Yeah, we haven't really talked about it. And I think actually just to shout out to the LACTLD guys, they have reached out proactively to me, and I've spoken a couple of times to the LACTLD membership. And within the ccTLD world, we're lucky with our regional organizations, obviously, I'm very much involved in Center, and if we could do more to exploit existing mechanisms for our work, we do get quite good recognition, I think, from the community, but it's

a bit of a patchwork quilt and we could be more tactical about that probably.

CLAUDIA RUIZ Nick, we have a hand.

NICK WENBAN-SMITH Okay. Thank you. Ah, again. Welcome.

VIVEK GOYAL Thank you. And I'm not sure if this is done already, but it would be great to see case studies from ccTLDs on what they're doing to combat abuse, the rate of abuse, the types of abuse that they see in their running the ccTLDs. Because every time we try and do something on DNS abuse, we keep getting questions like, where's the data? Where's the proof?

And you cannot boil the ocean every time to proof to somebody that DNS abuse is there and rising. But if it comes from ccTLDs, which are not bound by normal ICANN laws, it'll help very much for the whole community to use as a data point to further the course of fighting DNS abuse in ICANN. Thank you.

NICK WENBAN-SMITH No, thank you. And that's a very nice segue to the point I always like to make. It's a shame not more government people are here, but it's a fact or it seems to be a fact that the level of DNS abuse in ccTLDs is about 110th that you observe across the gTLDs. Now,

why is that? And nobody, I think has got the magic source to explain that, but there's some great work being done in ccTLDs, we perhaps have closer-- there's a more natural link between the ccTLD and the law and jurisdiction and the law enforcement community of that place.

So, is it more aligned because we're working in cooperation with the law enforcement authorities in the thing, and we're more, I suppose, naturally, we are more specifically looking at our own law and jurisdiction because that's the ccTLD, right?

Whereas if you're gTLD, you're doing it across the whole world and there's a patchwork of different laws and jurisdictions and so you're not necessarily aligning on that. But I do always like to say what a good track record the ccTLDs have. We have had, and this is I think one of my other, I wouldn't put it as strong as a complaint, but the way that the ICANN meetings are structured.

We have the different swim lanes for the GNSO and the different swim lanes for the ccNSO, and we have had many sessions in the CC world, in the ccNSO, which the Gs are not there for because they're in a different room where we have had exactly what you said, some great case studies from ccTLDs. We had Singapore the last meeting or the meeting before, meeting before, talking about specific issues around this event happened.

And the event intervention they took, and this is the great result that they had as a real case study about fraud in their jurisdiction

and what they did, how it affected the registry and the steps that they took.

And I think Monday where we are having .eu, .uk, and .us who are going to present to us about specific use studies involving AI and helping to remove abuse in their ccTLD, different ways of doing it in different ccTLDs, but that's exactly what you're doing to talk about it more, the success stories and things that are doing for everybody's benefit. Exactly that.

So, that's a really good discussion. I think we'll take away the inputs to what we should talk about over the next 6 to 12 months. So, what I like to do as chair of the committee is to have a sort of forward-looking work plan over the next 6 to 12 months on a continual basis. We talk about some things, we move forward, we then have the session like this with little introspection, like what's the next thing to do, which is right, and then we'll build something among those programs.

So, it was very interesting to compare and contrast the ccTLD community with the not ccTLD community to see whether there's differences in why that is and explore that. Because what we want to do is not create policy, but we want to also showcase good stuff for the non ccTLD community as well.

So, we're still doing really well for time, so we're getting like a long lunch break at this rate. But maybe I'm gonna snatch defeat from the jaws of victory. So, just looking forward then to the rest of the meeting, which is the slide, I think right near the end. Yeah, that

one. So, here we go. That's today, 25th of October, Monday I've talked about this a number of times, so if I talk about it again, maybe people remember it, and then there's the visual there, three till four.

There's a joint session between the ccNSO Tech Day and the DASC specifically looking at AI tools. And we've got hopefully addressing the point I referenced previously about AI being the number one priority. There's a specific session on AI, different ccTLDs presenting on the use of AI in the context of DNS abuse detection and prevention and mitigation.

So, should be super interesting session. And then on Wednesday, we have a joint session with the GAC. The GAC, I think, have an ongoing like prioritization list and I'm pretty sure that DNS abuse is always like in that list. It's always like the number two or number three thing. And they specifically want to talk to the ccTLDs about DNS abuse.

So, there are several sort of coffee point stations with a clipboard where ccTLDs are gonna talk about DNS abuse in different jurisdictions and have a sort of quite informal interaction with GAC members who can move between different places and talk to different ccTLDs in a less intimidating format than the sort of the full banquet room where you have to stand up and talk before everybody. So, that's sort of a safer place for GAC members to talk to any ccTLD about abuse and to sort of do that in a nice non-

threatening way. But obviously, it's an open session. Everybody is welcome to that as well. Any questions?

Great. Any further thoughts? So, contrary to-- well, let's move on to, I'll maybe speak too soon. I was gonna say contrary to perception, I'm not somebody to carry on talking for as long as the time allows, and we can finish early. So, if we go onto the any other business slide, I'm very happy to open the any other business slide.

Next slide. Oh, call for volunteers. This is a call for volunteers. There's always room for more. It's a really great group I think that we've got here. It's very inclusive, dare I say kind of fun. It's a serious subject, but we try to enjoy ourselves and to create good collateral and engaging sessions for the community. So, always looking for more people to join. Joke.

JOKE BRAEKEN Thanks, Nick. There was a question in the chat, which David already answered, from Serena, whether DASC membership is open to the public or only to ccTLDs. Maybe that's a good point to refer to right now.

NICK WENBAN-SMITH What was the answer to that question?

JOKE BRAEKEN DASC is indeed open to ccTLDs only.

NICK WENBAN-SMITH Okay, thank you. I thought that was the answer, but I thought we're also really inclusive, and you don't have to be a ccTLD to be like an observer. So, you can join and participate pretty much on an equal footing even though you're not technically a member. We are not difficult about that sort of thing. David, sorry.

DAVID MCAULEY Nick, I put an answer in chat, and I'm glad I got it right. But you're right, we do have observers, especially at meetings like this in our working sessions month to month, it's pretty much just us.

NICK WENBAN-SMITH Yeah, thank you. You are right. Okay, good. So, is there any other business or anything else that anybody would like to say on the topic of DNS abuse? I'm also happy to take feedback, as is Bruce, very happy to take feedback if you would like to give us feedback whether constructive, critical, favorable about the work of this group, makes bad choice in shirts or whatever. We're always very open to having that sort of dialogue and discussion. I think it's part of the beauty of this community is it's very open and level playing field.

BRUCE TONKIN It might be worth just mentioning that we're meeting with the GAC this week as well.

NICK WENBAN-SMITH It was on the thing, but it was on the thing. Yeah, I've already done that. Bruce pay attention. So, yeah, so the GAC session, I've spoken about. Martin Seaman, you've gotta say something. Say something funny and interesting. I saw you. Okay. Pablo.

PABLO RODRIGUEZ Thank you. This is Pablo Rodriguez for the record. I would like to propose that we should also include people from academia specifically because in the areas of computer science, there are lots of conversations about theory and cybersecurity, but there is very little policy discussion with the exception of my colleague who may be able to do the same in her university.

But it seems to me that the academic community doesn't talk much about this type of topics, and we should include them first to create awareness, and second, because we can also influence through that channel in one way or another, thus, reaching out to the prevention of abuse and other things that may relate to fraud. Thanks.

NICK WENBAN-SMITH No, thank you. And I think that's a really interesting observation, firstly. secondly, I don't know if you're aware of this already, and Rowena knows this, we have a good friend and colleague, Maciej, who's at Grenoble University, and he provides the academic rigor around some of the analysis for this sort of stuff.

And I'm very happy to reach out to him. It's been some years since he came up with his paper on analysis for measurement of abuse. And I think it'd be quite interesting to hear from him a bit more about the academic rigor and study that goes into it at the university level because there's other universities I'm sure who are doing this now. It's an emerging subject and it's would be interesting to get presentations from people like that. Olga.

OLGA CAVALLI Thank you. Thank you very much. This is Olga Cavalli for the record. Thank you, Pablo, for mentioning this. By the way, let me tell you that I'm leading the National Defense University. So, I was called by the Minister of Defense to include cyber defense and cybersecurity issues into the programs of defense, which were not so strongly included in the curricula of the-- by the way, we have three new careers and one is cyber defense. So, thank you, Pablo, for that because we need more activity and involvement of academics in this field. And thank you, Pablo.

NICK WENBAN-SMITH Yeah, I think the cybersecurity thing is sort of not necessarily in our wheelhouse, but it is probably more important than DNS abuse in terms of the vulnerability of the actual infrastructure. So, yeah.

PABLO RODRIGUEZ If I may, similar to Olga's program, we have a program in our university called Information Systems and Electronic Fraud

Investigation, and this is one area in which I would absolutely love to integrate this type of discussion in our program as a whole in specific courses as well. So, that would be quite interesting.

NICK WENBAN-SMITH: No, those are great suggestions. And I think we should maximize the brain trust. There's a lot of smart people, let's make them make use of the resources and thank you for that. I'm sorry, my friend from PG.

RUSSELL DEKA HARADA: Thank you. My name is Russell Deka Harada, I am .pg ccTLD manager from Papua New Guinea and also ICANN84 Fellow. My question is the same as Prof. mentioned, this cyber security, cyber defense capacity building program for developing nations, especially Pacific countries.

So, we are very weak, but always this cyber threat are happening, especially our finance related activities, our tax collectors, government tax collectors office, all the hack and attack, and also our Department of Finance, national government, they face this problem. Once this something happening, then people are panic and seeking assistance. So, prevent than cure is very important, but how your developed nation to assist our developing countries. Thank you.

NICK WENBAN-SMITH Thank you very much for that intervention. And I think the whole purpose, if you look at our charter, is to help people by providing resources, sessions, socializing things. There are many free resources in the community for, say, abuse prevention and measurement and these sorts of things and start to help.

But I think we're, yeah, as a CC community, we are acutely aware there's a lot of small developing countries with quite small infrastructure and resources and we should be always reminded that actually part of our role is to provide that sort of help to those sorts of places who don't have the scale or the long track record and financial resources to do that like some places do.

I think we do that by, we provide the volunteers and the leadership team to try to get these things talked about and to provide exactly what you've said, the community with the help that it needs and advice to deal these things. So, Rowena, did you want to say something earlier about Maciej and his work at the University of Grenoble, or has that moment passed?

ROWENA SCHOO I think it was just generally supportive. The moment has probably passed.

NICK WENBAN-SMITH Thank you, fine. Are there any more Zoom comments? Any more… Oh.

JOFAN YU

Okay. Thank you. I'm Jofan Yu from TWNIC. So, in addition to the internet community, like ccTLD, but also like cybersecurity expert, they also have a lot of discussion on this, especially they can share a lot of intelligence or something because they are their expertise. So, do we also think to include like I know like at first, I mean this association, they also have like the committee on DNS security as well and they also do some research on this, so maybe it's also good to include or invite them to do some sharing as well.

NICK WENBAN-SMITH

No, thank you, Jofan. So what I think is that this is a really important topic, but also what I think of it, that this is separate from the DNS abuse topic. This is more about cybersecurity and infrastructure security more generally, and I don't know if there's any of my colleagues here from council, whether that is something that we want to look at in terms of cybersecurity for ccTLDs.

There is the TLD ops group, which already looks at the technical levels in terms of, I remember they did a disaster recovery and planning session. I don't know, I'm not so close to those guys who are more on the technical side, whether they do cybersecurity workshops, awareness, that kind of stuff. I don't want to kind of tread on somebody else's toes if it's already going on in a different place, which I'm not in. Bart will correct me.

BART BOSWINKEL I won't correct you. I think it's one of the topics, so the internet governance group, cybersecurity, so it might be useful to look at them first, and that's more a governance perspective. So, that's another perspective you have till the ops is really focusing on disaster recovery, business continuity. So, more internal focus than external focus like cybersecurity. So, it might be an area maybe to expand your mandate.

NICK WENBAN-SMITH Well, it'd be more than doubling of the existing mandate I'm worried about. So, I'm not saying no, that's not my thing, but I don't think it is. Well, it's an incredibly important area, it's the number one priority for my organization. I know that's the thing we put the most investment into in terms of refreshing hardware and software and all the rest of it. This is the number one priority which keeps my--

BART BOSWINKEL In that sense, it's more, so it more would be more into the mandate or to all the ops expanding, not just disaster recovery business. It's more part of business continuity, isn't it?

NICK WENBAN-SMITH Yeah, I think, sorry, just off the top of my head, from memory that the TLD ops background came from things like sort of DDoS attacks and that kind of stuff, and [01:18:50 - inaudible] slightly different now, which is general threat in a world where a lot's happened in

the last few years. It feels like we're close to out and out hostilities between different nation states and it's a real issue that infrastructure is being targeted and that includes the ccTLD infrastructure and DNS.

BART BOSWINKEL: What is interesting is that you see from your perspective, I don't know about other ccTLDs whether they have that same experience to go through the same experience as you do is one of the interesting things, and I said that this morning as well, say, from the Finance Working Group, that group gutted some data about the diversity of the community, the ccTLD community, and that's very interesting and fascinating.

That might be an area or, say, the data to use to check whether, say, your perception or your perspective is shared across the community and valid. But it's a way to look at it. Let me give you an example. If you look at the distribution, say, of the domain names under management, you will see that the larger ones are predominantly private organizations. So, with their own responsibilities and accountability mechanisms.

If you look at the smaller ones, the vast majority, I would say, almost half is government related. So, you have a little bit of different perspective, different roles of the ccTLD manager as well and responsibilities. So, it is a way of looking at it, and look, it's definitely a serious problem, or yeah, it's your number one priority,

	but the question is whether it's a priority of others as well. Maybe it should be, but that's something to look into.
NICK WENBAN-SMITH	Well, it's not really for me to make that decision, but maybe I can ask, say, Peter and Jordan as the two counselors are in my line of sight, whether say, for example, council would be amenable to, in the same way that we do the survey for DNS abuse, maybe there should be a survey on cybersecurity for ccTLDs and whether that's something that is worth looking at in a bit more detail because it's come up here in this forum. But I think, yeah, I would want to get some sort of guardrails on what that looks like from Council.
BART BOSWINKEL	And maybe together with IPOC.
NICK WENBAN-SMITH	Yeah, or maybe.
CLAUDIA RUIZ	Peter has his hand up.
NICK WENBAN-SMITH	Peter first, and then Jordan.

PETER KOCH

Yeah, thanks, Nick. This is Peter Koch for the record. Of course, I can't speak for Council, my experience is that when discussions start to collude or combine cybercrime and cybersecurity, both sides lose because it's hard to focus. And I would strongly recommend against adding the aspect of cybercrime to an existing committee and the question of whether to this existing committee that already deals with cyber-crime in the widest sense, whether there's a home for that in either the TLD ops.

I don't really understand the conect to IGLC, but let's discuss that, or the topic would be addressed in another way. There's lots of experience in the regional organizations. Center for example, has founded or spun off an information, excuse me, sharing and analysis center in ISOC. So, there might also be lots of stuff at the region level to leverage on, but personally, and again, not speaking for council, I don't see that topic in this group. Thank you.

NICK WENBAN-SMITH

No, and what about doing a survey to see whether there is unmet needs in the wider community? We have, obviously, there's lots of sort of small ccTLDs for whom is a major issue and they don't have the resources to deal with it, and they're looking to raise it up the agenda in some way. Jordan.

JORDAN CARTER

Jordan Carter, .au and one of the council members. I think it would be an interesting topic to discuss in the council to see if there is

appetite to that. I don't know what the answer would be, but I think you'd be willing to just be careful in specifying what it is you're trying to find out.

So, getting the problem statement clear and how a survey could help with that. And I was also gonna make the point about the regional organizations to see if they've already done surveys along these lines and see if there's any information to share on that basis.

NICK WENBAN-SMITH: Yeah, thank you. I should know the center's position on this stuff, and there's a huge amount because we have a center group on security more generally, not just cybersecurity. So, we have got our, in the European region, I don't like to talk about regional stuff so much, but we are in Europe at least, so I can talk about it.

But we do, in the European region at a CC level, have an awful lot of collaboration and we talked about the ISAC, and in the last couple of years, we've really moved forward a lot, I think, on the security agenda. And maybe it's addressed, but I don't want to go off and follow various things unless I've got a mandate to do it from Council.

And I want to probably do it with eyes open as to what the global thing is as opposed to just a couple of data points in a meeting before we set a few hairs running for what it's worth. Great. Well, that was an interesting and unexpected diversion. I think that's it.

Thank you, everybody, for attending. Thank you very much for a lot of engagement actually.

And I didn't follow through on my threat to pick people out at random and make them do something interesting, but be on your toes because next time-- and Martin, it's not too late. There's three minutes left. Okay. With that, I'll wrap the meeting up. Thank you, everybody, and see you next time.

[END OF TRANSCRIPTION]