ICANN68 | Virtual Policy Forum – Plenary Session: DNS Abuse and Malicious Registrations During COVID-19
Monday, June 22, 2020 – 13:00 to 14:30 MYT

MARY WONG: And for that, I'm going to ask my colleague Ria to kick us off, Bruce. And after that she will turn it over to you and off we go.

BRUCE TONKIN: Excellent. Thanks, Ria. Go ahead.

MARY WONG: Hello, everyone. I think my colleague Ria is on mute. So if I can ask our techs to make sure that her mic is not muted.

And welcome, everybody, again. And we will do a restart. But the recording is still on, I believe.

RIA OTANES: My apologies, everyone. Can you hear me now?

BRUCE TONKIN: Yes.

RIA OTANES: Perfect. Hello and welcome to the plenary session on DNS abuse and malicious registrations during COVID-19. My name is Ria Otanes, and I

am the remote participation manager for this session. Please note that this session is being recorded and follows the ICANN expected standards of behavior.

During this session, questions or comments will only be read aloud if submitted in English within the Q&A pod. This feature can be accessed from the Zoom toolbar. I'll read questions and comments aloud during the time set by the chair or moderator of this session.

If you would like to ask your question or make your comment verbally, please raise your hand. When called upon, you will be given permission to unmute your microphone. Kindly unmute your microphone at this time and take the floor. State your name for the record and the language you will speak, if speaking a language other than English.

This session includes real-time transcription and interpretation. To view the realtime transcription, click on the closed caption button in the Zoom toolbar. To hear the interpretation, you will need to download the interpretation application. More information can be found in the session details on the events schedule and instructions are -- will be included in the chat.

With that, I will hand the floor over to Bruce Tonkin.

Bruce, please go ahead.

BRUCE TONKIN: Thank you, Ria. So this session is really a follow-up to the session that we held at the ICANN meeting in Montreal in November last year. Much has really changed in the world since then, particularly changes in, I guess, the way we're all working on a daily basis. Most of us working from home and probably most of us sitting at home during this ICANN meeting.

Last year we heard about the current obligations in the registrar contracts for receiving and investigating reports of DNS abuse and the requirements in the registry contracts particularly related to monitoring and reporting and maintaining statistical reports on the degree of which there's abuse in the top-level domain and the actions they're taking to address that.

ICANN Org itself also has a system of DNS abuse activity reporting with the acronym DAAR, D-A-A-R.

We heard about an initiative at the last session from, at that time, 11 registries and registrars to develop a framework for dealing with DNS abuse that both defines DNS abuse and sets expectations about how abuse complaints will be treated by some registries and registrars as well as how some might also deal with a narrow set of types of website content abuse.

We heard that the Competition Consumer Trust and Consumer Choice Review team also had a definition of DNS abuse that's a little broader.

We heard from a government representative about some common types of abuse that they are seeing at the last meeting.

And then there was a long conversation amongst both panelists and community members through the open mic. And there's a full transcript available of that discussion from the last meeting.

I think the sort of outcomes of that session included the need to better define terms and be clear about what ICANN is responsible for, so being clear on what the definition of DNS abuse are and have an accepted definition across the community.

The need to help people find the right parties that are able to address the different forms of DNS abuse that we see.

That take-down processes need to have appropriate appeal mechanisms. So there's an ability for people to appeal if a domain name was taken out of the DNS.

Approaches -- there were quite a bit of discussion at the last session about different incentives that could be used, perhaps put in place by registry operators to provide best practice amongst registrars.

There was a discussion about the role of contracts versus best practice approaches to the problem.

Certainly the contractual level, that there's appropriate tools available for the ICANN compliance team to be able to take action against parties that are operating in bad faith.

So as a follow-up, this session has been scheduled for the virtual meeting here at ICANN68. And we really divided it up into two components. The first component is to hear what's happened since

we had this discussion in Montreal, particularly in a very different work environment caused by COVID-19 restrictions with many end users accessing Internet services from home that are, perhaps, less secure than the services that they would access through either their workplace or their school environments where they're probably using computers and devices that have got current operating systems and various anti-virus, anti-malware.

What we are seeing now is a lot of people using end user sort of home devices and operating from home in perhaps much less secure environments. And so they may be a lot more susceptible to various forms of DNS abuse than we have previously seen.

So we want to hear from the panelists about, since Montreal, what's been happening, what seems to be working, and what's clearly not working.

And then in the second session, we want to hear from panelists about what they believe would be concrete next steps that the community could take that could be easily implemented and that would also have a tangible impact on the problem.

And then after that, we'll open to the audience for feedback from the audience and also questions from the audience for the panel.

So at this point, I'll hand across to our first speaker, which is Jim Galvin from the Registries Stakeholder Group. Over to you, Jim.

JIM GALVIN: Thank you, Bruce. I'm Jim Galvin from Afilias, representing the Registries Stakeholder Group here.

Next slide, please.

All right. And there we go. So there are two important points that I want to make here about DNS abuse. I think the first one here is to point out the DNS abuse framework. It's a voluntary framework that exists. Afilias joined a number of other registries and registrars to be a founding member of this, and quite a number of us have signed up to honor and respect this DNS abuse framework.

And its most important point here is the definition of "DNS abuse" as represented in that framework has actually been officially adopted by the contracted parties, both registries and registrars. So this does good for the community. It provides a very clear baseline on issues that the contracted parties as a group, as stakeholder groups, agree are elements that they should address directly when they are encountered in the DNS system.

In fact, DNS abuse is clearly defined in five broad categories of harmful activity insofar as the intersect of the DNS. That's with malware, botnets, phishing, pharming, and spam. And what I want to do is call out spam in particular because it's really a slice of spam. It's not about spam in and of itself because that's a whole separate topic all by itself. But it's about spam when it's used as a delivery mechanism for these other four forms of abuse. And that's an important distinction to draw.

So, you know, we're not as contracted parties taking up the obligation to address the spam problem. We want to deal with DNS abuse and what it represents.

The second point here, as we move to the next slide, is it allowed us an opportunity to draw a clear distinction between website content abuse and DNS abuse. Spam is similar to website content abuse in that it really is a step beyond what registries and registrars ordinarily in control of. We ordinarily have control of the registration system.

And you can see here one of the things that's in this framework is a description that shows that there are many players in this ecosystem of DNS and website content abuse, beginning with site operators over on the left-hand side. So you have got website operators or service providers of various sorts.

And then you've got the registrant, of course, who's making use, using their domain name, to create those kinds of sites and those opportunities. And a hosting provider that is part of this process, that they are also using.

And a registrant, of course, you know, gets their services from a reseller or a registrar. And then the registry.

The DNS abuse definition that was provided in the previous slide very clearly provides to the DNS actors on the right-hand side represented here in green, or the outer box being dashed. And, you know, registries or registrars very clearly promptly investigate and address those kinds of abuse.

But the important thing is that we only have that one very blunt instrument for dealing with abuse. And that is a take-down; that is removal of the domain name from the DNS. And that's the role the registries and registrars play. When abuse is more content-related, then you usually want a more surgical kind of mitigation to be applied. And that's where you really do have to have access to that content. You have to look at it, make an assessment, and you have to do something to a website or to the service in order to remove that abusive content.

And we're going to be hearing more about it here today with COVID, since that's one of the things that we're really supposed to be talking about here, is abuse in the presence of COVID. COVID provided a nice example of how this abuse framework and this representative ecosystem can work very effectively.

We've already had one session here earlier today in ALAC. The GAC had a presentation about this. Registries and registrars, the contracted parties had a Webinar back on June 11th. You can find the recording for this available on the rysg.info website. But we talked a lot about the fact that the COVID-19, the registration abuse, the DNS abuse was actually quite limited. In fact, nonexistent for all practical purposes.

The only reason that actions were taken -- and the number of actions were taken were quite limited -- were because of addressing content abuse. And the DNS framework allows for that. Rather going at this

blunt instrument, sometimes the right thing to do is to start over on the left.

And we do our part. As registries and registrars, we've done our part to reach out to hosting providers and such in -- to the registrars, reached out to hosting providers, to deal with content abuse to where we could. Or if it was an absolutely egregious representation, bad data, and that was the sole purpose of that website, then we applied our blunt instrument of doing a take-down. Otherwise, we would have handed it off to the party that's more relevant to that process.

So those are my two important messages in this presentation in this panel. Let me turn it back to you, Bruce. I look forward to being responsive to questions as they come up. Thanks.

BRUCE TONKIN: Excellent. Thank you for that summary, Jim.

Over to Graeme Bunton who's a representative from the Registrar Stakeholder Group.

GRAEME BUNTON: Good evening, Bruce.

BRUCE TONKIN: Good morning.

GRAEME BUNTON: Yeah. Pleasure. Thank you for having me.

Maybe first a caveat, I apologize. It's kind of late for me here. I haven't had a haircut in a very long time, so I'm wearing a hat for a very sensible reason.

If we could go forward a slide. Please and thank you. Maybe another one. Great.

So, first, I think thanks to Jim from Afilias. Yes to all of what he said. I'll try not to cover too much of -- a lot of the stuff that he was talking about.

But, you know, registries and registrars have been strong partners in a lot of this DNS abuse conversation and a lot of the activities around COVID. And so I don't want to duplicate that work. But just know everyone, that registries and registrars are very aligned on that message that Jim was sharing.

I wanted to take a few minutes to talk about some of the activities inside of the RrSG since ICANN66 in Montreal.

I will speak a little slower. Thank you, Mary.

So out of Montreal, it became clear that we needed to really dig into DNS abuse. And so we created a subteam inside of the Registrar Stakeholder Group to begin tackling this issue. We've been meeting every two weeks since Montreal with some exceptions for holidays.

And that took a little bit of time for us to work out our working methods for that group. There are things we need to be able to talk about in that space that were sensitive. And so ensuring that we could have and build that trust was really important for us. And then sorting out the priorities for the stakeholder group in the myriad of DNS abuse issues that we could be touching.

We made a deliberate choice as we were starting to try and do a lot of external education and provide some documents and resources to the community as a whole because it really felt like there was some low-hanging fruit there, some education that we could provide that would be beneficial.

So to that end, we put out a guide to abuse reporting best practices. And I've seen this document referenced in the wider community a number of times. And it's really just if you found abuse of some sort and you think the registrar is the appropriate place to deal with that abuse, then this is the information that we would need in order to act on that abuse.

And so my sense is it's been really useful. I know that it's been used by European law enforcement as a basis for a similar form of their own.

We also created a minimum required information for WHOIS data requests document, and this is, in some sense, similar to the previous one, which is if you require registrant information that is no longer public because of privacy regulation, then here is what you need to

provide to a registrar in general to submit a fully formed request. And it's no guarantee, of course, that you would get the outcome you're looking for, but it's helpful information.

So all of these are available on the Registrar Stakeholder Group website, rrsg.org, and I'll put that link in the chat.

And then we get to a bit of COVID-19 related activity. So it became clear to registrars relatively quickly that this was a new and exceptional circumstance, and so we, you know, pretty quickly got together and put together some of our best practices or things that we've learned. Tried to put out a statement we thought would be helpful for the rest of the industry.

And, you know, since then, I thought we'd made some really good progress, and I don't want to reiterate too much of what Jim was saying and I would also reference the contracted party session that we held -- I think Jim said it was the 11th. (Indiscernible) no meeting anymore. I assume it was in the past two weeks.

But there I shared some data and some of the approaches that were brought to the table during COVID-19.

I will say that, you know, like you've heard a number of times, the material amount -- or there was not a material amount of DNS abuse. There was certainly an awful lot of COVID-19-related registrations.

We had within the stakeholder group, I thought, some really good internal discussion, sharing of approaches, sharing of tools, sharing of

lists. And those lists were really important for people who didn't have the capacity internally to begin assessing all those integrations themselves. And those tools were -- or those lists were also wildly varied in quality, and that was a really interesting challenge for us.

I will say, and I really heard this clearly from Laureen and Gabe in the GAC session earlier this evening about really good interaction and communication. And we found that was really helpful from our end and appreciated the openness and willingness to dialogue and work together that LEA brought to the table.

We're now in a process of summarizing some of that data, some of those experiences. We'll have another RrSG statement coming out hopefully in the next day or so.

This is sort of front-running the next session of this plenary, but there's a real opportunity here to sit down and do a -- some pretty serious work on what worked, what didn't, what are the gaps, you know, what are the lessons we can really learn from this crisis, and how can we use that to inform the industry.

And I think with that, I'll pass it back to you, Bruce.

Thanks.

BRUCE TONKIN: All right. Thank you, Graeme. And our next panelist is Laureen Kapin from the Government Advisory Committee and also the Public Safety Working Group within the Government Advisory Committee.

Over to you, Laureen.

LAUREEN KAPIN: Thank you, Bruce, and welcome, everyone. I am an attorney at the Federal Trade Commission where I focus on consumer protection law.

Next slide.

And you'll see my little disclaimer. These are my comments, not necessarily the official position of the FTC.

My other role in the ICANN universe is as co-chair of the GAC's Public Safety Working Group.

Next slide, please.

I wanted to share with you some information that the FTC has put together regarding COVID-19 complaints. Just sort of highlight the scale of these issues.

I do want to emphasize this is general information about COVID-19 complaints, probably just a portion of which would relate to DNS abuse. But I thought it would be helpful to get some information on the scale of this issue. My agency collects complaints from consumers not just in the U.S. but from around the world, and then we have lots of information available to the public on what we're collecting and what we're seeing.

And you'll see this graphic shows our current totals of complaints are over a hundred thousand, and that is just from January. And you can

see in the squiggly lines to the right that these complaints reached a high point in April, but they're still fairly high. The level of money lost in terms of fraud cases is in excess of $68 million, and the average consumer loss is $289. And you'll see that this relates to COVID-19 and also stimulus money. In the United States there's been the big program to provide money to support people who are now out of work and don't have income coming in. And of course with every benefit, there's also opportunities for fraud. So I wanted to give a sense of the scale of this problem in terms of the complaints we're seeing.

Next slide.

I also wanted to point out that in terms of communication methods for how scammers and fraudsters contact people, you'll see that phone is the number one method, but right there at second and third are via websites and via email. And of course those can be related to abuse of the Domain Name System.

Next slide, please.

I want to emphasize first what's working well, because the second part of our discussion is going to focus on the tougher issue of what can be improved. But as -- as Graeme noted, and which I do want to emphasize, law enforcement has worked really well with registrars and with ICANN to be able to collaborate when domain names seemed inherently deceptive or possibly related to troubling content. We were able to have a dialogue with registrars to refer these aspects and have a direct channel to make these referrals and follow up. And those

open channels of communication were very welcome and very effective. And that's a great example of how we can work together to combat DNS abuse.

We are aware that several of the registrars actually were proactively screening the registration of domain names that related to COVID-19, and when they saw having troubling they referred things back to law enforcement. So this was really a two-way street, and that two-way street was really effective so that we can refer things to registrars and registrars can refer things to law enforcement. That type of cooperation and especially that proactive screening was a great example of things that were working well in the area of DNS abuse.

And with that, I'll pass the baton over.

BRUCE TONKIN: Thank you, Laureen.

It's always good to hear that something is working.

LAUREEN KAPIN: [Laughter]

BRUCE TONKIN: And I think we've got Peter Van Roste from the Country Code Name Supporting Organization. I'm not sure if we've seen him yet. Are you there, Peter?

PETER VAN ROSTE: Hi, Bruce. I'm here.

Thank you so much. My name is Peter Van Roste. I'm the General Manager for CENTR. We're the European ccTLDs.

What I'm going to talk in the next few minutes also is reflected in findings from my colleagues from the other regions. So LACTLD and APTLD and AfTLD shared similar observations on a webinar two weeks ago.

Importantly, I mean, I think most of the people on this call will know that ccTLDs are not part of the abuse framework. ccTLD policies are drafted on the local level and not within ICANN. But we've been asked to share what we observed during COVID, and there is very -- there are interesting parallels between these two worlds, but pretty much alike.

So we looked into COVID-related abuse. Within the CENTR community, a sample of 12 ccTLDs provided us with rich datasets from January to April. 750,000 registrations. So small and large registries were in that group. .8% or 6,100 domains were COVID themed. So that is what, from the limited amount of things that we can see in a domain, we can at least check the name for COVID, coronavirus, et cetera. So keyword based.

Of those 6,000, only a quarter, 1,600 names, were high-content names. So other than parked for sale or simply no nameservers functioning.

Of those thousand 1,600, a handful got confirmed in the different ccTLDs that participated as being used for malicious practices, confirmed by the competent authorities. And to my colleagues from Nominet, the signal three in U.C. and six in D.K. So -- And that works -- that is the same findings as what our colleagues from gTLD world found out.

What did not go well, I think we failed very soon in the game to get our act together on the stats. There was lots of noise from outside industry, even in the popular press, that there was a -- that the problem was significantly higher than what we eventually found it to be. We lost valuable time in that. I think we're still having the discussions with some of our partners, governmental agencies, law enforcement agencies, on zooming in on what really needed to be at the focus of our attention.

What did work well, the work together with local authorities, whether they're national health authorities, consumer protection authorities, or law enforcement. I mean, that was really the key to finding, zooming in and fixing those names that were being used for malicious purposes.

Overall, and as conclusion, so what did ccTLDs do in this COVID period? And more in the broader context of how could one compare that to the abuse framework.

So there was more -- there were checks upon registration. So these extraordinary circumstances, especially for smaller ccTLDs, required a

lot of work, but they looked into the registrations manually and some of them did it automatically. They checked for accuracy, and they worked on accuracy. Registrants, in close collaboration with registrars, but registrants were chased to improve the accuracy they were providing. And the third point, which I already mentioned as one of the things that really worked well, is the collaboration with local authorities. That to us was really the key.

That's it. Thanks.

BRUCE TONKIN: All right. Thank you very much, Peter. It's always good to get both a Generic Top-Level Domain and a Country Code Top Level Domain perspective. Interesting to see that there are a lot of commonalities in what both types of top-level domains saw.

The next speaker that we have, which is the last speaker in this segment, is Jonathan Zuck from the At-Large Committee -- At-Large Advisory Committee.

Over to you, Jon.

JONATHAN ZUCK: Thanks, Bruce. Good to be here. Thanks for having me.

Go ahead to the next slide. Try to be efficient. There's so many of us. I see 39 panelists listed.

So I just wanted to talk a little bit about the end user perspective on this and question the idea of whether or not this was a nonserious event from the standpoint of DNS abuse but also at the same time suggest that our conversations need to take place in parallel to a crisis like this taking place, right?

So it's not a question of if this is all about COVID or not. It's generally about bad actors and things like that, that we need to go through.

So this particular statistic is from Check Point Software. And statistics can be crazy. But, basically, they did a search on COVID-related domains; and they're more likely to be abusive registrations than nonCOVID-related domains.

That's all that means, Reg. Thanks for your question.

Next slide.

Just an example of a phishing attack that took place in Italy. It was an email that went out and hit all kinds of Italian organizations. Said: "Due to the number of cases of coronavirus infection that have been documented in your area, the World Health Organization is prepared to document that includes all the necessary precautions against coronavirus infection. We strongly recommend that you read the document attached to this message."

And, of course, this doctor doesn't exist. If you open the Word document and follow the instructions, it installs particularly

pernicious malware on the machines in a place that was already suffering from a lot of difficulties during the crisis.

So I don't want to minimize what happened during the COVID crisis. I think that this session is more about attacking this problem in a holistic way. And I think we're still dealing with the issue of systemic abuse by a few actors. Folks have said that DAAR reveals it to be eight actors. If we know those eight, we need to figure out if there's a way to address those issues in a way that is acceptable to the good actors that we all know and love from the ICANN community. That's really where the At-Large is focused.

Thanks. I'll pass it back, Bruce.

BRUCE TONKIN: Thanks, Jonathan. So what I think we'll do is we'll jump into the next session just in the interest of time.

I do notice there are a few questions starting to form in the Q&A. So we'll address those after we've heard from the remaining speakers.

The remaining speakers is really -- we've heard a bit about what's happened since Montreal, what's working, what's not working. And, really, the purpose of the next set of speakers is what can we actually do about it. What's something concrete we can do that would make a difference?

So with that, I will hand it over starting with Mason Cole from the Commercial Stakeholder Group of the GNSO, or Generic Names Supporting Organization.

Go ahead, Mason.

MASON COLE: Thank you, Bruce. Hello again, everybody.

I want to start off by applauding the contracted parties and what they've done so far in relation to the COVID problem. It's been admirable to see all the good actors to do that. But what we're facing is a situation where if DNS abuse wasn't a problem, we wouldn't be having this conversation. So with that, next slide, please.

So some quick facts about DNS abuse. We all know that it's a chronic and growing problem. It occurs year after year. And as we've seen with COVID, it's magnified by outside events like natural disasters or the civil unrest we're seeing in the United States right now. But the common theme is that the DNS is leveraged for illicit purposes.

Next slide, please.

Some facts about DNS abuse: It's steadily growing. You can see that by 2021, it's estimated that cybercrime is going to cost the global economy more than $6 trillion in damages. And that's a real problem. It's not all related to domain names, but a lot of it roots itself from domain names.

And I pulled a stat here from the National Association of The Boards of Pharmacy where they talk about specifically how abusers are leveraging the DNS for the benefit of rogue pharmacies. And you can see that many of these domain names are clustered in safe-haven registrars, which is a practice that we all see when the bad guys are trying to hide.

Next slide, please.

So looking back a couple of years, we see here a common trend when there's a significant world event. In this case, it was hurricanes. And you see a spike in registrations of hurricane-related names, and not all those are going to be trustworthy names.

Next slide, please.

And here's what we saw with COVID-19. So you can see the same sort of spike, and then it levels off and starts to decline a bit.

Next slide, please.

And here's what I talked about earlier. There's some ongoing civil unrest here in the United States. And you can see that there are trend lines on domain names being registered related to the issues involved in that unrest.

Next slide.

So I reached out to a couple of companies to talk about what actually happens when the DNS is being abused in a way that's detrimental to

them. And I received some information from Microsoft that you can see here: That COVID-19 has resulted in an increase in the efficacy of same-type cybersecurity attacks than in the past. And because -- this was mentioned earlier. But people working outside their company firewalls are on devices that aren't well-managed, and you get password spray or other brute force attacks. Again, many of those can leverage the DNS for problem behavior.

In fact, I found out from Microsoft that between March 16th and June 10th, they investigated more than 30,000 domain names that utilize COVID-19. And approximately 14,000 of those names were flagged for follow-up.

I also found out some information that's not in this presentation here, but I found out from Microsoft -- or from Facebook, excuse me, since March for them, 261 domains have been detected that include combinations of Facebook core products in COVID-19-related terms. Names like fbcovidcare or covid19facebook.com. So you can see it's an ongoing trend.

Next slide, please.

So the exacerbating problem is that ICANN Org doesn't have the tools it needs to combat the behavior via rogue registrars. We all know that the good guys are in this room and they're doing good things. But the bad guys are outside the room, and we need to do something about them.

So the result then is this tragedy of the commons where everybody is incentivized to do not as much as they could because not enough people are held to account.

Next slide.

So what can be done from here? Don't address one scam at a time reactively. We've seen trend lines now that repeat themselves, and we can learn from those past and current abuse behaviors to take proactive steps to address abuse before it happens, not after everybody has been harmed.

So we can also implement real tools for combating abuse and make those tools apply across the board. The voluntary efforts are fantastic, but we need help with the people that aren't in this room.

So we can take tools that look like -- oops, sorry. Can I have the previous slide? Thank you.

So we can look at tools like the registrars' response to the United States Congress, which was active and helpful, and institutionalize that process and memorialize it in contracts. And we all know that most big players in here are doing the right thing. Again, it's a small group that bears disproportionate responsibility and we need tools to hold them accountable. That's it for me for now, Bruce.

Back to you.

BRUCE TONKIN: Thank you, Mason.

And our next speaker is Jeff Bedser from the ICANN Security and Stability Advisory Committee, or SSAC as it's often called.

Over to you, Jeff.

JEFF BEDSER: Thank you, Bruce. As was said, this is Jeff Bedser with iThreat, a member of the Security and Stability Advisory Committee.

And next slide, please.

So SSAC has an active work party on DNS abuse. And, basically, we believe that the community is now at a point where we can say definitively we have an agreement that the abuse of customers or consumers of the DNS is a problem. It's being addressed across multiple facets of the community. And sessions such as this are showing a lot of progress.

So what we're looking at is can we come up with a framework for effective practices for abuse resolution, not just amongst contracted parties but across the entire DNS ecosystem? Can we come up with a model that actually reduces victimization through quickly addressing abuse when it's determined and evidenced?

Next slide, please.

So as mentioned prior by other speakers, such as Jim Galvin and Graeme, the categorizations of abuse and definitions of abuse are

pretty well established now, at least on the technical abuse side. What types of content abuse may need some more work as far as determining if there are broader groupings under content abuse?

One of the things that certainly needs more progress is the evidentiary standards amongst the community in the DNS ecosystem. Each player, each party, tends to have a different standard for what they find appropriate evidence to demonstrate abusive domain. And that evidence may come very much in handy when you are basically asking a party to break a contract with an end user who registered a domain or backup stream. So evidentiary standards are going to be very important to standardize a best practices model.

Effective abuse reporting practices also are something that we're looking to address in this work party because the abuse-reporting practices do have to have a commonality of -- when you have a certain type of abuse worth the first STU contact. Who owns that particular type of abuse to take care of it, to get it resolved, get it resolved quickly?

So mapping that out in a model that allows for a reporter of abuse, whether that be a consumer or that be a law enforcement entity or any type of other abuse entity, knowing where to go with that complaint and going back, of course, with the right evidence to demonstrate that type of abuse.

And then additionally, what we believe is there should be escalation paths. Escalation paths can also be progression paths, if you will,

where you're looking to understand if a certain party that is the right party to address this type of abuse does not respond, refuses to respond, your goal here again is to reduce victimization and to allow the quick resolution of an abusive domain. So what is the escalation path? If it fails at one point, where does it go to next? And how is that handled?

And then, of course, it leads to reasonable time frames. If you have a party that does not respond, what is a reasonable time frame to go back to the upstream part of the ecosystem and ask for assistance getting this abuse resolved if you do not have a response?

And this comes down to comments I've seen both in the Q&A as well as in the chat sessions where you're talking about there are parties that are signers to the framework that are very dedicated to getting things resolved. And there are plenty of players in the ecosystem, as Mason's mentioned, where there are safe havens. And it's very easy to get your abuse registered and used because they are protecting the abusers by making it very difficult to contact them or get things resolved within.

So that does take us to the last part of this content we're trying to resolve, is the availability and quality of contact information within the ecosystem. If you don't -- obviously you've got registrant data available in some forms but that doesn't necessarily who you need to contact to get something resolved. It may not be the registrant. It could be the hosting company. It could be the CDN provider. It could be the mail provider. All these abuse sit on different parts of the

ecosystem. And the availability of adequate contact information to assist in getting a rapid resolution of an abusive domain is very key.

Bruce, I will pass it back to you.

BRUCE TONKIN: All right. Thank you, Jeff.

And I will introduce now Brian Cimbolic from the Registry Stakeholder Group.

BRIAN CIMBOLIC: Thanks, Bruce. Hi, everyone. My name is Brian Cimbolic. I'm general counsel at PIR, and I also oversee our anti-abuse program.

Next slide, please.

So looking forward, you know, sort of the theme of this second part here, I think there's a few things that we should focus on. First, I think continued dialogue between contracted parties and other stakeholders in the ICANN community are really important. I think people have said it's a shame that all this COVID -- the work between registries and registrars and law enforcement happened, but it's a shame something like COVID had to spur it along.

And I think that might not quite be a fair statement. There's been, especially in the last five years, a really great track record, in my opinion, of cooperation between law enforcement and registries and registrars. Things like the security framework for registry operators to

identify security threats, that was a jointly drafted document between PSWG and registry operators. There's a child sexual abuse material discussion group founded by a number of registries and registrars that really seized the input and wisdom and experience of a number of law enforcement agencies and child sexual abuse material watchdog agencies, and the framework to address abuse.

Those were all things that happened because there's a real desire on the part of contracted parties, or at least many contracted parties, to identify and work on the problem. There's not one thing that work -- that inspired either of those three initiatives in the same way that COVID-related work did. So I think just those sort of continued dialogues as well as the ongoing discussion with the SSAC I think is really helpful.

The more that we understand one another's pain points, one another's limitations, the less I think we're likely to speak past each other, which often happens in these settings.

Second, so Jim pointed out that the framework has -- the framework to address abuse has sort of grown quite a bit. We started out with a handful of registries and registrars, grew to 11 registries and registrars prior to Montreal. And now we're up to north of 50 registries and registrars that have signed on and committed to the definition of DNS abuse and committed to take action upon recognizing DNS abuse as well as certain categories of identified website content abuse that is so egregious that the registry operator or registrar will take action, things

like child sexual abuse materials or human trafficking or imminent threats to human life.

The last one I think as far as paths forward is getting creative. What can a registry or a registrar, maybe not across the entire DNS but within the registrations that flow through it, what can it do?

And one such example, if you can go to the next slide, please, is something -- it is not a Registry Stakeholder Group initiative, but this is something that at PIR we've developed and launched and we're very proud of. It's called the quality performance index.

And what this does is it provides financial incentives to registrars for good registration patterns.

And what is a good registration pattern? We look at a number of things such as abuse rates, renewal rates, domain usage, DNSSEC rate, SSL usage, and basically just domain usage.

The reason "abuse rates" here is bolded is because recently we made abuse rates how -- when I say "abuse rates," I mean the registrar's percent of abuse creates relative to its overall creates. If it doesn't map -- hit a certain threshold, then it just is automatically disqualified from participating in the promotion.

So it's a -- really it's a carrot and a stick. It rewards registrars that have low abuse rates and high-quality domain name usage. And it's a stick insofar as that registrars that don't meet those criteria are unable to participate.

And we've seen some registrars come to the table that really may not have been the most proactive on abuse before. But because they know they're missing an incentive that others are getting, they've come and asked us to help work on how they can get better at abuse.

So one last thing I want to say is that this is something we are proud of. We think if any other registry operator would be interested in adopting or using QPI, we are happy to talk you through and help you implement whatever version of this that works for you. We think it makes sense. Also, wholesale registrars, this model might work for you.

So we think that this is something that can really help drive positive behavior. So, look forward to having those conversations with other registries and registrars as well as anyone else that has questions about it. Thanks very much.

GRAEME BUNTON: Bruce, I think you're muted.

BRUCE TONKIN: I am, indeed, muted. Thank you, Brian. Over to you, Graeme, just to give another perspective from the Registrar Stakeholder Group in terms of what can be done going forward.

GRAEME BUNTON: Thanks, Bruce. And I'll try to keep this pretty zippy.

So moving forward, I think going back to the work inside the Registrar Stakeholder Group, we're finding now that, a), we need more time, and b), probably more resources. It's difficult, certainly during the pandemic, to get the material amount of time we need to get the work done. And so maybe there's some room there for us to reach out to GDD or ICANN staff to see if there's ways that we can work together to get some of the output we would like done, done.

More broadly speaking, though, around DNS abuse in general, I think sort of the clear line that we have drawn around what is DNS abuse, at least for the Contracted Party House, I think is a really important first step. You know, I was doing some research around, you know, data, trying to find real quality data around DNS abuse. You know, this checkpoint blog from Jonathan Zuck is a really example of ba- -- good -- example of bad data. It's limited and doesn't really dig into the issue materially, and so, you know, that's a problem. But I think what we can do now is we've got an industry definition. Let's go and gather some clear data. From there, I think what we really need to do is we can get a real sense of the attributes shared by the bad actors that everyone likes to talk about. Who are they, what do they do, how do they do it.

Once we've identified those attributes, then what we can do is figure out what tools and solutions we need from there. But I think we have to start at that point.

Thanks.

UNKNOWN SPEAKER: Muted.

BRUCE TONKIN: Sorry, Graeme.

Thank you, Graeme.

Over to you now, Laureen, from a Government Advisory Committee perspective.

LAUREEN KAPIN: Thanks, Bruce.

And I'll ask to advance to slide 5, please.

Rut-ro!

Slide five of my slides. There we go. Room for improvement. Perfect.

And just as a preface, I want to pick up on two points made by the two J's, James Bladel and Jonathan Zuck, in the chat. James had observed that a lot of the conversation seems to be about rules for the bad guys. How do we figure out rules to convince the bad guys or -- or deter the bad guys. And Jonathan Zuck pointing out that the other part of the equation is what proactive measures can be taken to basically screen out the bad guys, you know, from step one. And I think that sword-and-shield approach is actually a really useful concept.

So in terms of room for improvement, some of the things that we can use as a shield are these dedicated channels for law enforcement to deal with abuse and security threats, and certainly the COVID-19 issues have shown us that, you know, if we have specific contacts that we can -- that we can communicate with quickly to deal with things in a nimble manner, that that is a great -- a great tool to have in our arsenal.

Another really important concept, and again, this falls into the shield category, is making sure at the outset that the data that's being collected on those who want to register domains that may or may not be involved in abusive activity, that that information is accurate, because what we've seen is that when this type of verification is going on in an effective way, that the bad guys and gals are going to want to go elsewhere. So if there's a rigorous program in place, that can be, again, a real deterrent, a shield.

Turning to the sword, one thing that is needed is clear, enforceable contract obligations. Certainly the current contracts, especially for new gTLDs, are a very good start, but we think that they can go further. There needs to be more than just obligations to put provisions in agreements that prohibit DNS abuse. There need to be provisions that outline what steps need to be taken and what are the consequences for failing to take those steps. It's only when the contract obligations reach that clear and enforceable threshold and that level of specificity that ICANN compliance actually has the tools it needs to engage in robust enforcement activities.

So on the -- on the sword side, that's a real direction that we need to go in.

Next slide, please.

So in terms of -- in terms of a wish list. This is when Laureen gets to take her magic wand and transform the world the way she would like it to be. It would be beneficial if there were incentives to encourage good behavior. And we saw an example of some carrots that Brian discussed, but we need more carrots, folks. What incentives can we have to encourage good behavior. Perhaps these could be financial incentives. There are other types of incentives as well. But certainly incentives to ensure domain name accuracy before the sale of a domain name, that would be a great thing to encourage and reward if people are achieving very high rates of accuracy.

There should be more scrutiny given for bulk registrations. There may be some valid reasons for bulk registrations, but if there are bulk registrations, that should be a yellow flag to inquire further. And that extra level of scrutiny could serve to screen out bulk registrations that may be intended for malicious use.

Another thing on my wish list, and this is reflected in some of the CCT recommendations that deal with how to deter systemic abuse occurring in certain registries or in certain registrars, would be a no-fly list for registrants that repeatedly engage in abusive behavior. Again, you have to have accurate registrant information to be able to do this. But if there is a registrant that's been identified as continually

engaging in illegal conduct, then that registrant should be really under scrutiny for being able to register a domain name.

So those are some of the things on my wish list and ways that we could improve the ecosystem.

Thanks so much. Passing the baton now.

BRUCE TONKIN: All right. Thank you, Laureen.

And our final panelist is David Conrad from the icann.org.

DAVID CONRAD: Thank you, Bruce. I'm David Conrad, ICANN's Chief Technology Officer.

Next slide, please.

So the question was asked, you know, what can ICANN Org do. And I sort of broke this down into tactical and strategic. Tactical is sort of near-term things that we can do, just sort of more -- sort of thrust in the same directions that we've already been heading.

One of the efforts that we've undertaken recently is something that we call the Domain Name Security Threat Information Collection and Reporting Tool, and that's what we used in the context of phishing and malware distribution for the COVID-19-related domain names.

And the intent of that tool is to provide high-confidence reports to the registrars so that they can take appropriate actions. And, you know, we track and report on the outcomes of those actions.

That tool we built primarily for the COVID-19-related effort, but it's something that could be applied in sort of similar situations moving forward where for -- you know, some event occurs, we can identify domain names associated with that event and then track to see if there's a surge in abusive uses of the domain names, at least for phishing and malware distribution.

One of the things that we're working with the community, and particularly the Registry Stakeholder Group, is to try to refine the DNS abuse activity reporting tools reports. Right now, the -- we've been publishing those reports for I guess about a year or so, but there's still sort of a lack of understanding of what the data actually means and what its limitations are. And there have been numerous requests for more detailed data, different statistics, different ways of collecting up those statistics. So that's something that we're planning on doing in the near future.

We've already started including ccTLDs into the underlying DAAR infrastructure. Of course that's voluntary. The ccTLDs that have expressed interest, we've worked out an MOU with them and they provide the necessary data into DAAR. And we're looking to figure out how to add those into the DAAR reports. That's a little complicated because since the ccTLDs are voluntary, it's likely that a ccTLD will be -- that's doing a good job will want to see themselves in the report,

whereas one that's not doing such a good job won't bother, whereas the gTLDs are sort of required to provide the data that we use for these reports.

We're also still looking at how to get the registrar data incorporated into the DAAR reports. That proves to be challenging because of WHOIS rate limiting. We're trying to figure out ways around that but it is proving to be a pretty gnarly challenge.

And with DAAR, it actually is a tool that can provide you, as the community, with information about anomalies. And one of our efforts internally has been to identify those anomalies and then go out and talk with them and try to figure out how we can help address the reason that they are anomalies within the data.

If you look to the graphs that are there on the right, you can see a -- the things that I've circled with the red are anomalies that, you know, they're clear outliers from the basis of the other domains. And there's some reason for that. You know, it may be for financial reasons, it may be policy reasons. But we actually have had some success in going out to the registries that are showing up as anomalies, talking to them, understanding what those issues are -- their issues are, and helping them to address them.

The DNS Security Facilitation Initiative is a project that we're spinning up. The intent of this is to provide a clearinghouse of information, an ability to collect best practices and promulgate those best practices throughout the community, focusing on how to improve DNS

ecosystem security in a broad context, not just at the registry and registrar level but in general across the DNS ecosystem as a whole.

Within the context of compliance, we're looking at proactively enforcing the relevant obligations. You know, compliance addresses complaints and conducts audits focused on DNS abuse using data from various sources. They -- Obviously compliance is aware of the DAAR reports, is able to obtain similar data, but there's also data that they have access to, the complaints that are filed, and all of that has a signal effect that you can identify sort of outliers based on those signals and perhaps, you know, target audiences based on those outliers.

In terms of strategic, ICANN Org looks to facilitate the ongoing discussions regarding DNS abuse. Clearly there needs to be clarity in the roles of the registrants versus contracting parties versus ICANN.

One of the constant requests we get is for ICANN to act outside of its bylaws, to do things that we are expressly forbidden to do. And obviously we can't do that, but that leaves the complainants, the people who are suffering at some form of abuse, without, you know, much alternative. So one of the things that we're looking at is to provide more information resources to allow those people that ICANN cannot help, for whatever reason, to have someplace that they can go to to pursue their complaints in a way that hopefully will get them some sort of benefit.

As you may have seen, we have announced a couple of MOUs, the MOU with cert and the MOU with GCA. And these are part of an effort we see as sort of a long-term effort aimed at partnering with anti-abuse organizations, law enforcement, and others to try to help facilitate communications between law enforcement and those who can take actions, registries and registrars, to also provide more information about the role of ICANN and what it is we can and cannot do.

But ultimately, you know, whatever the community has a consensus about is what, you know, the organization will end up doing. You know, obviously if we're required to enforce the contracts, which is what we do, unless the obligations are clearly written and understood, they tend to be unenforceable. One of the challenges that we have had is the differing interpretations of the contracts, and what some people see as clearly abusive is not what other people see as abusive. So that's one of the things that we hope to eventually clear up with the community's help.

And with that, I will hand it back to Bruce.

BRUCE TONKIN: Okay. Thank you, David.

We've got a few participants in the attendee list that have got their hands raised. Perhaps we'll go first to Lori Schulman. You had your hand raised. And if staff could unmute Lori to ask her question.

LORI SCHULMAN: Yes. Bruce, my question was answered in the chat. I was really concerned about phrases like "low rates of abuse" and "nonmaterial rates of abuse" and how they're being measured because what I'm hearing from my members, trademark owners that we're seeing spikes, and that to a point that Margie Milam made in the chat is what's happening is the word COVID, COVID itself is not being registered but COVID is being attached to brands as well. And that's highly concerning, concerning for the brand as well as for the general public concerned about COVID.

BRUCE TONKIN: Okay. Thanks, Lori.

Move to the next person on the list with their hand up, Georgios Tselentis, if I've got that last name right.

Georgios, if you would like to go ahead.

If we can unmute it, if Georgios is able to ask his question.

Okay. I'll take one more person in the cue with their hand up. Jannett, J-a-n-n-e-t-t, if you would like to ask a question.

Okay. Perhaps we'll jump to one of the questions in the online forum. I believe staff will read that question now out. Is that correct, Ria, or would you like me to do that?

RIA OTANES: I can read the question, Bruce.

BRUCE TONKIN: Thank you.

RIA OTANES: From an anonymous attendee: Q to the previous speaker: Have the agencies considered the possibility of designing a secure process to actually channelize the relief disbursements through the perhaps making use of existing and new DNS technologies such as a blockchain-based payment gateway, not only for the U.S. but usable elsewhere?

LAUREEN KAPIN: And I think that one was for me, and actually I was just typing an answer to that in the chat in the Q&A pod.

My agency is not involved in the distribution of relief payments, so I can't speak to that. What I can tell you is that it's been widely reported that some of the systems used, and I think your question gets at this in terms of these payments were susceptible to -- to people getting confused. For example, the envelopes were perceived to look like junk mail, so they were thrown out, or folks were contacted allegedly by people who said, "We have your stimulus money but you need to provide us with some verifying personal information first," and of course that led to personally identifiable information being given away, which puts folks at a greater risk of identity theft.

So I don't have the specific answer to your question, but I think the implication is that perhaps more thought should be given to how these payments are made so that they can be made in a way that makes them less susceptible to fraud and deception.

BRUCE TONKIN: Thanks, Laureen. We will take another question from the question and answer written forum. I think the question is from Fabricio.

RIA OTANES: Question from Fabricio: Voluntary measures are a good start but not the long-term answer. How do we ensure that some registrars don't carry the weight for all and level the playing field through proactive data-driven contract compliance? Seems as though through contract compliance, we address those bad actors we are all talking about that are, quote-unquote, not in the room.

BRUCE TONKIN: That's probably a question for you, David, which is: How would you use the data that you have to assist contract compliance?

DAVID CONRAD: So my group's responsibility is to create -- to collect and publish unbiased fact-based information for the community to facilitate policy discussions within the community.

Compliance has access to that information, just like everyone else. The information that we have is made public as much as we're able to based on the agreements and those sorts of things.

In the case of the DAAR data, clearly those outliers that I showed in that graph, which I believe is Figure 13 in the DAAR report, identifies something odd is happening. That information can be taken by compliance as part of the proactive compliance effort that I had mentioned and speak with those registrars or registries, in this case, to try to identify what the issues are that are resulting in the anomalous behavior.

It doesn't mean that the registry is necessarily a bad actor. It simply means there's data indicating that there's something odd going on. And it's useful to try to identify what that oddness is and try to mitigate it.

BRUCE TONKIN: Thank you, David.

We'll go back now to the list of people with their hands up. So I think -- I tried Jannett before. Maybe I'll try another time, if Jannett has her hand up. J-A-N-N-E-T-T. The mic is open if you would like to ask a question.

Okay. I will move to the next person which is Luisa Paez. So L-U-I-S-A P-A-E-Z. Your mic is open if you would like to ask a question. No? Okay.

And I will go to the last person who has their hand up, which is Arasteh. A-R-A-S-T-E-H. Your mic is open, if you'd like to ask a question.

No? Okay.

One more try. Steph Viljoen, your mic is open if you would like to ask a question.

KAVOUSS ARASTEH: Hello?

BRUCE TONKIN: Hello. Yes, go ahead.

KAVOUSS ARASTEH: Can you hear me, please?

BRUCE TONKIN: Yes, I do. Go ahead, please.

KAVOUSS ARASTEH: Okay, good. Good morning, good afternoon, good evening. Just a question irrespective of the accuracy of the data related to the DNS abuse and so on and so forth, what are the areas in which we have not been yet successful to combat this abuse?

And what are the reasons for that and what we can do for that?

And associated with that, are there coordinated and harmonized action throughout ICANN with respect to combating against the area in which we have not been successful and a coordinated plan to do that? Thank you.

BRUCE TONKIN: Thank you, Arasteh.

I think a few panelists did speak on that, and it will be in the transcript.

Does anyone want to add further to what they said earlier on what's not working and what to do about it? Any of the panelists?

LAUREEN KAPIN: This is Laureen. I want to thank Kavouss for his question.

If we only had a great answer to that very important question, we would all have a clear path forward.

What I will point out is some of the very useful information that was recognized in the study commissioned by the Consumer Trust Review Team that pointed out that there are -- and this was also mentioned in the chat, that there does seem to be a concentration of bad behavior in terms of DNS abuse among relatively few registries and registrars and that we need to do better in figuring out how to both identify and then act to prevent systemic DNS abuse by the same repeat players, so to speak, recidivists. This would be a great place to be able to start.

And, indeed, the CCT review team had some very specific recommendations in that respect, particularly that there could be a process to challenge registries and registrars who were havens for DNS abuse and that there could be a process then to have them explain why there are such high rates of abuse within their systems and why they are failing to address it. So that would at least be one small step that could be taken.

BRUCE TONKIN: Okay. Thanks, Laureen.

We'll now take another question from the online question and answer forum, I think from Susan Payne. If you'd like to read that out, Ria.

RIA OTANES: From Susan Payne: Laureen, we have talked in the RPM's PDP about the no-flag concept in the context of repeat cybersquatting, e.g., using X number of URS/UDRPs. But there are challenges with how you might effectively implement this. Do you have views on how this could be done?

LAUREEN KAPIN: It's also a challenging issue. I think, first, you have to start with data. You need to make sure that your information about your registrants is accurate and you're not dealing with a bunch of fake information or fake aliases.

And then I think there would need to be agreed-upon standards for what constitutes bad conduct that's going to constitute a strike, for example, if you have a three-strike system.

So certainly this isn't something that would be -- that one would be able to implement without both good data and then agreed-upon standards for what constitutes bad behavior to the extent that that individual or entity should no longer be entitled to the privilege of registering a domain name.

But these are certainly steps that could be taken assuming that the community engaged in the work of both ensuring that the system has good, accurate data and then coming up with sensible, reasonable standards of what constitutes bad behavior sufficient to exclude an entity or an individual from being able to register that domain name.

So the short answer is it can be done, but it certainly would take work and analytical discussion and good data.

BRUCE TONKIN: Thanks, Laureen.

Over to you, Ria. I was going to say we have another anonymous question. Another question -- well, go to the anonymous question, I think, because we've had one question already from Fabricio. So there's another anonymous attendee question.

RIA OTANES: Okay. Anonymous attendee: The previous panelist talked about shield approach, but the wish list was restricted to what data is collected and its accuracy. Why not shield users by having safeguards about who the domain name goes to? At least names such as curecovid.com, imaginary, which have a high propensity for abuse for, e.g.

LAUREEN KAPIN: I would agree with that suggestion. There certainly could be proactive measures taken to look at domain names that carry within their name a message of deception.

And one of the things that I will applaud some of the registrars for doing is looking closely at the registrations within their system that gave them cause for concern.

I know that's very resource intensive. And I know, indeed, it's very hard to do that in an efficient way that doesn't require a lot of resources, although I'm hopeful that systems can be developed to make it a bit easier.

But I think that that is certainly something that also could be put into the shield category, looking at domain names that carry in it an implicit message of deception because those are the types of things we don't want to see registered in the first instance.

BRUCE TONKIN: Okay. Thank you, Laureen.

The next question is for Graeme from an anonymous attendee. So I will let you read that, Ria.

RIA OTANES: To Graeme: The 2013 RAA required ICANN's work with registrars to identify and implement cross-field validation tools. Cross-field validation is common, automated process used worldwide. We just heard that many ccTLDs are using it to help combat COVID abuse. Will registrars finally implement cross-field validation per the RAA? Why or why not?

GRAEME BUNTON: [Laughter]

Thank you for the question. I don't know that I can answer this definitively, certainly not on behalf of all registrars in this particular moment.

The short answer is that it's more complicated than you think it is. We have global businesses that operate around the world. And geographic applicability of cross-field validation is not as robust as you think it is.

People's cottage -- like, I have some inlaws who live in something called Willow Cottage with Bucalay (phonetic) in Jersey in the Channel Islands, and it doesn't work. And we need a global solution.

But this is probably not the place to really dig into that one materially. Suffice it to say it's complicated.

BRUCE TONKIN: Okay. Thank you, Graeme.

Does anyone else want to comment on that? It's come up a little bit, I think, in your comments as well, Laureen, about accuracy.

Does anyone else want to comment about the sort of WHOIS data accuracy issue as it relates to helping at least identify who to contact in the cases of abuse? No? Okay.

MARY WONG: Bruce, this is Mary from ICANN Org. I believe one of our panelists, Jim Galvin, has -- would like to speak to that or perhaps to another point.

BRUCE TONKIN: Go ahead, Jim.

JIM GALVIN: Thanks, Bruce. Jim Galvin from Afilias.

I've been thinking about this question as it relates also to data accuracy. But we were having a discussion about where we've been successful and where we've been unsuccessful and what our challenges are for the future. And I think there are two points that I'd

like to just put on the table for discussion, two challenges for us to think about.

As we think about what we can do to make the system better, I think it's important to understand that we don't have a single system for enforcement within the system. And I'll focus on registries for the moment, as an example.

So consider that we have gTLDs and we have ccTLDs. The mechanism by which we might get a uniform standard of behavior between those two broad categories is quite different. So it's interesting that a lot of our discussion here, I would say, seems to focus on what we can do with gTLDs to make the world better and then at the same time we talk about ccTLDs that have implemented particular data accuracy rules and, thus, they have affected in a positive way the presence of abuse. And so those are just sort of two different categories of things.

And I think that's a challenge we have to keep in mind as we think about standards of behavior that we're looking for.

And then the second point that I would make in the standards of behavior, especially as we think about looking for thresholds of abuse or, you know, looking at its presence in general, the discussions about DAAR in particular, one of the things that's really important here is you don't control the bad guys. We don't know who the malefactors are. We don't know where they'll appear, when they'll appear, and what they're going to do.

And so what's interesting is the actual presence of abuse might indicate nothing more than the fact that that's where the bad guys went that day. Tomorrow they'll go somewhere else.

The fact they might have abuse today and abuse tomorrow doesn't mean it's the same abuse in those two days. And so the fact that my level might not change might indicate absolutely nothing except that a second set of bad guys came up and executed abuse.

I think that those are two important challenges to keep in mind as we try to find these black-and-white rules that are going to help us manage abuse in whatever form, both on mitigation side and on creating standards of behavior. Thanks.

BRUCE TONKIN: Thanks, Jim.

I think I will sort of wind up then with a bit of a summary so we finish on time. But I'd like to thank all the panelists for describing sort of what they're currently seeing and have seen over the last few months during the COVID-19 pandemic and also the helpful suggestions for how we can, I guess, make it easier to report abuse and also get action taken against that abuse.

We heard, for example, from Jeff from the Security and Stability group that they're working on essentially a set of tools and processes around how to report abuse, what needs to go into an abuse report, what would be considered timely response to an abuse report, et cetera. So

I think the more some of these best practice approaches can be documented the better.

The registries, registrars, the two stakeholder groups, have agreed on a definition of DNS abuse. I think that's helpful because they're the practitioners. They are the ones that are typically receiving these reports.

We heard from Brian talking about some of the things that some of the registries are looking at to incentivize good behavior. We heard from Graeme talking a bit about needing some more resources to further develop the systems and processes from a registrant point of view.

Laureen had mentioned that one of the things that really helps law enforcement is having the right context at registries and registrars where they can escalate and get prompt action. So I think we heard from the country code operators, for example, that the relationship between the registry operator in each country and the law enforcement agencies in each country have been working well in recent months, presumably because the parties know each other and know how to escalate.

It gets much harder to do that on a global scale. So, for example, if a person in a law enforcement agency in one country, how do they know the right contact for a registry or registrar that's in a different country?

Heard also Laureen sort of supporting the idea of incentives, supporting what Brian had mentioned.

Also, mentioned that one of the characteristics -- I think a few people are mentioning that. What are the patterns or characteristics that registries and registrars can look for and at least pull things out for further analysis? Perhaps seeking to improve the accuracy of information associated with somebody that's doing rote registrations or what otherwise looks like unusual activity.

And David talked about the data that ICANN has been collecting and out of that data identifying some outliers or registries or registrars that seem to have a high incidence of particular types of DNS abuse and working cooperatively with that registry, registrar to identify why that's happening and what steps they can put in place to combat that behavior.

So, again, I thank all the panel participants, particularly trying to focus on what we can do moving forward and what are the tangible next steps.

Also, want to support or thank all those that participated. I think we had up to about 440 people that are participating in this session.

Many people have been using the chat forum, which I think is a great way of people discussing the topics that the panelists have been raising as the meeting has unfolded. So that seems to be a good use of parallel time and allowing people to engage in the discussion as well as listen.

So at that point, I will close this session. Thank all audience members and thank all panelists. Thank you, all.

[Applause]

[END OF TRANSCRIPTION]