ABU DHABI – Cross Community Session: DNS Abuse Reporting for Policymaking & Mitigation
Monday, October 30, 2017 – 13:30 to 15:00 GST
ICANN60 | Abu Dhabi, United Arab Emirates

IRANGA KAHANGAMA: Good afternoon, everyone. If you want to grab your seats and fill in, we're going to get started here in a second.

Thanks.

All right. I want to thank everyone for coming in today, for today's session on abuse reporting for fact-based policy-making and effective DNS abuse mitigation. My name is Iranga Kahangama, I'm one of the co-sponsors of this event with the Public Safety Working Group here on the behalf of the United States Federal Bureau of Investigation and a member of the Public Safety Working Group.

My co-chair Cathrin, do you want to introduce yours?

CATHRIN BAUER-BULST: Sure. My name is Cathrin Bauer-Bulst. I'm one of the co-chairs of the Public Safety Working Group of the GAC and I'm with the European Commission.

IRANGA KAHANGAMA: Thanks, Cathrin.

So what I'm going to do is just give a very brief overview of the history and logic of this event and what we're hoping to get out of it, and then Cathrin will move into more of the logistics and details of the event.

So this is from the Public Safety Working Group perspective the natural evolution of a focus on DNS abuse and DNS abuse mitigation that we've tried to highlight for the ICANN community. It's a natural progression of other things that we've done, including asking various questions through GAC advice on DNS abuse issues, and a number of other conversations and events that we've had.

When the call came out for cross-community sessions, we were obviously very interested, and I think it became very clear that there was high interest within the community at talking more about this issue and moving the ball forward on how to go about addressing some of these issues.

So to give you guys a bit -- a very short background, we had three working group calls from volunteers from different stakeholder communities that you see at this table, and we were -- we tasked ourselves with determining how to go forward on this event.

The Public Safety Working Group initially had brought together the concept of principles around DNS abuse mitigation to try and consolidate around those.

After proposing some, it became clear that there are obviously lots of different perspectives on these issues, and so the natural result of this event became the fact that we should discuss these issues with a broad subsection of the community that you see here today.

So what we've done is we've put this event together and we've bucketed DNS abuse mitigation issues under three categories related to the identification of DNS abuse, reporting of DNS abuse, and statistics and how that data should be used.

So we're going to cue up the event for audience participation surrounding those three general themes, and we're hoping to drive towards a principle-based approach based on the outcomes of this event and the continued engagement of the Public Safety Working Group and the rest of the community.

Thank you.

CATHRIN BAUER-BULST: As we move to the next slide let me just introduce briefly. So we're first going to hear two short presentations by David Conrad and Drew Bagley who are sitting to my left from your perspective, and then we have a panel composed of representatives of the different groups, participants from the different groups who have been also contributing to the run-up to the session, to the preparation that Iranga was referring to. So we have Alan Woods from the Registry Stakeholder Group, and we have Graeme Bunton from the Registrar Stakeholder Group, we have Tania Tropina from the NCUC, Denise Michel from the business constituency, Jonathan Matkowsky from the IPC, Rod Rasmussen, the incoming chair of SSAC, and Jamie Hedlund, who is the V.P. for ICANN compliance and consumer safeguards.

Go to the next slide, please.

So as Iranga was saying, we are trying to structure this discussion, and so the way this session would run is we're going to start with two brief presentations, and then we're going to try to move the discussion through the three categories that Iranga has already identified. And what came out in the calls, in the discussion on the principles was that while we could not yet agree on what principles should apply for DNS abuse reporting for how we collect the data and how we then use it afterwards, it was clear that the principles that would apply to this process would have to respond to three key questions, and those are the questions that you find here on the slide and that we will come back to in the discussion after the two presentations to kick us off. And those questions are, first, how do we identify DNS abuse in a reliable way? Then on that basis, how do we create effective and transparent abuse reporting to make that data available? And then third, how do we then go on to use this data?

And those are the three sections that we're hoping to discuss with you today. So while we have a very large panel of renowned experts on the subject matter, we very much want to include you and have this be a participatory event.

So what we will do is we will have the two short presentations to kick us off. Then we're going to launch the discussion on each of the sections with a question to one of the panelists. And while we are responding to that question, asking it, we would invite you to already -- if you want to weigh in either on the general question that is asked for this category or on the specific question that we're discussing with the panelists, to please identify yourself to one of the ICANN staffers who are around here with mics. You see them holding up the numbers here, so please just stick up your hand. One of them will come and find you and signal to us that you would like to intervene, and we will make space for that.

In the interest of having as many opportunities for intervention as possible, we're going to limit the time for responses to two minutes for everyone. So that also applies to the panel. We're trying to be as equal as possible here. Please -- Please do intervene and please do share your views with us.

And now, without further ado, we will move to the first of the presentations which will focus on the domain abuse activity reporting system and which David Conrad will give to us.

David over to you.

DAVID CONRAD: Thank you very much.

I'm David Conrad, ICANN CTO. For the relevance to this discussion, we have been developing something called the Domain Abuse Activity Reporting system within my group and the office of the CTO.

Next slide, please. Oh, that's me. Hah! There we go.

So just a little background. What is the Domain Abuse Activity Reporting, or DAAR as we prefer to call it because it's much shorter. It's a system that allows for the reporting of domain name registration and abuse data across TLD registries and registrars. Right now it's focused on the gTLDs because that's where we had data that we could do analysis on, but the system is not necessarily limited to that. If ccTLDs would like to participate, we're happy to discuss that with them.

How does DAAR differ from other reporting systems? As I'm sure many of you know, there are a large number of reporting mechanisms out there, some of them -- most of them, in fact, are associated with sort of commercial products or services.

What we're doing is studying all the gTLD registries and registrars from which we can collect data. We -- Unlike most reputation -- or most analyses that are done, we try to use a large number of data sources, and these are reputation feeds, also known as blocklists or RBLs.

We also collect that data over a period of time in order to maintain sufficient data to allow for historical studies.

We tend to look or we're actually required to look at a number of different threats. The threats that we focused on are the ones that were identified in the Beijing GAC communique, and they include phishing, botnet demand and control, and malware distribution, and we also arguably, controversially, include spam in our analysis. We include spam primarily because it's a highly effective vector for the other forms of abuse, and it also provides an index and provides information to us because typically when a TLD is being impacted by malware of one form or another or malicious activity of one form or another, it will also be impacted by spam.

We also -- and this is sort of the key point -- are trying to take a scientific approach, being as transparent and reproducible as we possibly can. The genesis of the DAAR project was actually around the time of a report by a vendor of security hardware that showed a number of gTLDs as being 100% spam or abuse related, and some of those reports were sort of humorous in the fact that one of them was 100% spam related, and that zone consisted of one domain, which was a NIC dot top-level domain, but because the top-level domain happened to match a particular string that that security vendor was looking at, it was actually, I believe, .ZIP, that resulted in all the domains within that top-level domain as being classified as malicious.

When the press -- When that came out, the press actually sort of ran with it. It actually generated quite a number of questions, both to ICANN and to the community at large. Subsequent to that, a number of folks within the community came up to me and ICANN and asked us -- and actually said, "Well, somebody should maintain an authoritative list. Someone should produce a well-documented methodology that everyone can agree to so we don't get these biased reports that are generated by commercial interests."So that triggered the initial thoughts that would eventually lead up to DAAR.

Next slide, please.

It's me again. Jeez! Anyhow.

UNKNOWN SPEAKER: Do you want me to hold it?

DAVID CONRAD: No, I'll figure this out eventually. It's technology. I'm not good with that stuff.

[Laughter]

So I mentioned that DAAR uses many threat data sets. So we collect the same abuse data that is reported to the industry and Internet users. One of the key requirements of DAAR was that anything that we do with this -- this project should be reproducible by anyone. We are not relying on any confidential data. We are not generating any data ourselves. We're basically taking publicly available data and correlating it and basically simply generating big spreadsheets that document the abuse of various forms within various categories.

The abuse data that we collect is used by commercial security systems that are protecting millions of users and billions of mailbox on a daily basis. The academic and industry users are -- are making use of this information just as we are, and they trust these data sets. And academic studies and industry have validated these data sets for accuracy, global coverage reliability, and low false positives.

The structure that we came up with with DAAR was to have an extensible framework, and we're experimenting with doing analyses of different subsets of the data just trying to get a better understanding of what's actually happening out there.

The key point here is DAAR is a tool that allows the community, the ICANN community, to see how the domain name ecosystem is being perceived outside of our community.

See, I didn't say "next slide," and then it doesn't listen to me. I hate it when that happens. Here we go.

A question has come up about the criteria by which we select data sets. This slide shows the criteria that we're using within the current version of DAAR. One of the activities that we're undertaking is to request from SSAC their input on the criteria by which a feed will be selected for use in DAAR, and we're also right now developing, too, an RFP for the community -- sorry, for independent experts to provide input on our methodology. Once we receive that information back, we will produce a document that describes the methodology that we propose to use and submit that for public comment. That will then be fed back in as a normal ICANN process, and we will modify the data feeds according to the criteria that has been -- that input has been provided on.

But right now, the data sets that we use, the requirements for those are that the operational security communities trust the data set for accuracy and clarity in process. In particular, any data set that we're using has to have a very clear process by which a name is added or removed from the blocklist. The chosen blocklist must provide a threat classification that mirrors what we need. So the botnet, the malware distribution, the phishing are the primary ones.

And these RBLs are broadly adopted across the operational security community. These are feeds that are incorporated into commercial security systems, that are used by network operators -- for example, in mail servers and et cetera -- to protect users and devices, and are used by email and messaging providers to protect their users.

Just for clarification, on these reputation blocklists that we're using, they're actually used pretty much everywhere. They're in browsers, they're in cloud and content serving systems, they're in your social media tools, and they're very frequently in the DNS. In the -- where was it? In Copenhagen, we actually had a presentation during the Technical Experts Group by Paul Vixie of Farsight Security. They have developed software that makes use of something called response policy zones that allows for the blocking of domain names via policy.

We are aware of a number of Internet service providers and email service providers that are blocking entire top-level domains because they believe those domains are too full of malware -- malicious domains and DNS abuse.

In addition, private network operators use RBLs and commercial firewalls, and enterprise mail and messaging systems and third-party email service providers.

This is a list of what we're currently using -- and I apologize for going a bit over time -- within the DAAR system. So we have basically -- what is that? Seven sort of primary RBLs, and one of those is actually a composite list that has a whole bunch of additional ones.

So why is DAAR reporting spam domains? This is a question that has come up on a couple of occasions.

In the Hyderabad communique, the GAC had expressed interest in spam, and of course we always listen to everything our community tells us. More realistically, spam is a major means of delivery of security threats, and the DAAR system measures domain names that are found in the bodies of spam, not the spam domain themselves.

And with that, I will pass it back to Fabien, I suppose? Or Iranga or Cathrin?

Somebody.

CATHRIN BAUER-BULST: Thank you very much, David. Drew. You're up next.

DREW BAGLEY: Thank you, Cathrin. My name is Drew Bagley and I'm with the Secure Domain Foundation and CrowdStrike. And building off of Dave's presentation about the value of this data and the reliability of this sort of data, I would like to discuss how we can use this data instead of merely on an operational level to block TLDs, instead to inform policy that can actually help improve efforts to maintain a free and open Internet and not run contrary to the idea of universal acceptance, which is what happens when abuse goes unabated.

As Dave mentioned, there is consensus in the community with regard to certain forms of abuse, particularly with regard to phishing and malware, which are explicitly prohibited by agreements, and with regard to the common delivery mechanism used for them with spam.

And so what's important for the community to understand when working with abuse in a policy fashion is not to get caught up in all the different interpretations we can come up with for abuse that prohibits us from actually doing anything about abuse. Instead, it's very important as a community to begin working on policy issues where there is consensus and where there are measurable metrics. And as Dave described, there are many reliable measurable metrics with regard to phishing, malware and spam, as well as botnet command and control.

As part of the Competition, Consumer Trust and Consumer Choice Review Team, we looked at the problem posed by DNS abuse as it related to the safeguards put in place to prevent abuse in the new gTLDs. And to measure this as a proxy, what we looked at was phishing, malware, and spam, and commissioned a study to look at data similar to what Dave presented on various black lists and derive analysis from this in a macro-level way so that we could come up with policy recommendations.

And I use this as an illustrative example of how this sort of data can be used to actually drive data-driven policy-making in the community.

What we found as the result of a -- a one-year analysis that looked at this data was that, in fact, abuse was something that really was not completely universal in every TLD. And similarly, it was not random. Instead, we were actually able to identify factors that either were more likely to be correlated with increased abuse in a particular zone or with particular registrars or low levels of abuse with particular registry operators or registrars.

And so it's likely not surprising that in instances where there were increased registration restrictions and, therefore, it was harder to register a domain name, there was -- there were lower instances of abuse.

Similarly, registrars or registry operators who tended to have higher correlations with very high levels of abuse were also found to have very low-price offerings and often various bulk registration options, which I will get into in a moment.

And, also, when doing a very microlevel analysis in some of these TLDs, we found that there was a strong correlation between trademark terms being used as bait and phishing campaigns, which is likely not a surprise. But the particular example highlighted in this report involved 76 domain names that use different permutations of Apple trademarks such as iPhone to, you know, try to do a targeted phishing campaign against users. And those 76 domain names comprised 76 of, I think, 83 instances of abuse in that TLD during a specific quarter.

And as a whole, what the data showed us is that there, in fact, is a policy gap. And I think that's why it's very important what the DAAR project is doing and what others in the community are doing by being able to collect and analyze these large datasets, particularly relying upon WHOIS data because then you can actually see where, in fact, our existing mechanisms may not account for every sort of situation we're dealing with that may, in fact, affect the stability and resilience of the DNS.

So I'm going to highlight two registrars in particular that are very problematic with our existing tool sets and that should inform our policy making going forward.

The first is a registrar which has since been suspended but was able to operate for the majority of 2016 with very high levels of abuse. And, in fact, it was not the unabated high levels of abuse that led to its suspension. Instead it was at the of the day, they stopped paying their bills; and there were a few other things cited. But, basically, if you enable cybercrime, you should still pay your bills and then you might be able to get away with it longer I think is one of the lessons here.

What this really highlighted, too, was that when we are in a complaint-driven model where we are waiting for a reactive approach to DNS abuse, then we might actually go a while before those complaints come in and before we're actually able to do something about it as a community.

Whereas, if we're able to use these broad DNS datasets such as what the DAAR initiative will bring about and highlight for the community, then this is something where maybe we'll be able to detect problems beforehand instead of waiting for the specific violations to come in after so many victims will likely have been affected.

And here's the second registrar, AlpNames, which is still operating. Similarly, there are very high levels of abuse. Also, at the same time that the CCT research was done, this particular registrar was offering bulk registrations whereby a registrant could go to AlpNames and register 2,000 domain names at once and AlpNames would conveniently create the domain -- they had the domain-generation algorithm available for the users. So you could randomly generate 2,000 domain names which I'm sure had very legitimate uses and thereby have your domains registered. And not surprisingly, this registrar had very high levels of abuse but without actionable complaints coming in. Has not necessarily faced a suspension procedure.

And this is something where with this bulk data and insights we're able to gather, this presents a potential policy gap for the community.

I keep hitting the wrong button here, or maybe I just want to keep emphasizing those two registrars.

[Laughter]

So where we are with the -- by way of example of the CCT review team is we've been able to use this data and develop specific policy recommendations that will be released to the community in our draft DNS abuse chapter that should be available within the next week or two. But, you know, it shouldn't end with the CCT review team. Instead as a community, as we have more of this data available and transparent to the community, whether it's through DAAR or whether it's through members of the cybersecurity community such as APWG, Secure Domain Foundation, Spamhaus, Stopbad, where all these members are coming forward and presenting this data, we as a community should not merely use it operationally to block things but instead should use it to inform policy decisions, identify these gaps, and really make sure that we are able to switch from a reactive model to abuse to a proactive model, whereby registrars and registry operators make it more difficult for repeat offenders to continually abuse their services and also where we can use this data to measure progress and see if we actually are mitigating abuse in a holistic fashion. And so I hope that this panel today is able to really discuss this from different viewpoints because obviously this touches upon many areas within the community and this is something we want to get right.

Now that we're at a point where we have usable, actionable data, we should really use it and embrace it to create policies that will create a better DNS for all of us. With that, I pass the baton back to Cathrin.

IRANGA KAHANGAMA: Thanks, David and Drew for your presentation. I'm going to re-emphasize the two-minute max time limit on some of these responses. We're running a few minutes behind, but at least I want to make sure that there's plenty of participation.

So, again, I'm going to start the questions with some -- with the panelists and then after the response, anyone in the audience should feel free to grab one of the mics and join in on the conversation.

So I guess we'll start, perhaps, with Alan if he doesn't mind kicking off some of this. But maybe starting with the top of the -- I guess, of the chain.

We just heard Drew talk about certain instances. When you have a very obvious abuser, what tools does the registry have at its disposal to kind of convert some of these observed trends into repeat offenders or abusers to help identify some of these issues?

ALAN WOODS: Thank you, Iranga. Alan Woods. I'll just introduce myself. I'm from Donuts registry. To get straight into the question, I mean, you say "obvious abuser" and that gives me cold chills straight away because unfortunately -- you know, I see the data and we see the data coming through in things like DAAR. And it's from these sources that provide us with fantastic lists of things that are potentially abusive.

However, we are not sitting in a position where we can actually say that that is an obvious abuser because we still lack unfortunately the evidence that is underlying that, that we can action or we can elevate or escalate to the registrar or to the appropriate party to look into it.

So the first question we really need to ask -- and this is how do we know that this is an obvious abuse? I mean, we do use -- obviously when we do get information and we get evidence, obviously we then would use that evidence. We would put it together, we would objectively review it, and then we would escalate it to the appropriate party who in this instance would probably be the registrar on record.

And with that -- if the registrar does not take action, well, then, obviously the registry themselves would take -- well, consider taking action in that.

So at the moment, the tools available to us are, yes, we would look at the indicators that we receive via lists such as maybe Spamhaus or SURBL. But we then ourselves would need to find extra information, extra evidence in order to bridge the gap between a statistic and an actionable piece of evidence. And I'll pass it on, on that one.

IRANGA KAHANGAMA: Thanks, Alan. As a brief follow-up, would you say it's fair that at a minimum, these statistics are a good kind of way to point to something that may need further investigation to kind of aid the registry side?

ALAN WOODS: Yes. And to be I suppose somewhat controversial on that is to say that, yes, it would point us in that direction. But a lot of time, the only other evidence that we can find when we review that is the fact that it is listed on that blocklist. So we would like to be able to get that little bit more detail or those extra ways of finding the reason why they were listed as opposed to just a blank statement as to the fact that that was just on a listing.

So it's -- it's difficult for us. We try our very best in those instances. If we see a flash point, we do everything in our power to try and identify the reason behind that flash point. But that is not always the clearest thing. And it's very difficult to get that information, especially from those blocklist providers who don't provide us with that information because they can't or they don't have it or it's industry secrets.

CATHRIN BAUER-BULST: David, do you briefly want to come back to that?

DAVID CONRAD: Just to add one of the reasons that DAAR includes historical information is to actually help in identifying trends over long periods of time, including sort of abusive information over a long period of time. So I agree 100% that, you know, the concept of obvious abuser is most likely sort of in the eye of the beholder and additional information is necessary to identify a true abuser versus, you know, someone who has -- likes having random strings for a domain name.

But part of the effort that we're trying to facilitate within the community is to provide information, particularly over a long time -- long period, to enable policy discussions that help clearly identify trends of abuse within particular namespaces.

IRANGA KAHANGAMA: Thanks.

Next we'll have Rod chip in, and then we see mic Number 2.

ROD RASMUSSEN: Hi. Rod Rasmussen. For the record, I'm speaking in my individual capacity and not representing SSAC here.

I'm going to directly answer this question because I think the answer that we've heard has been an answer to how does a particular entity identify abuse in a reliable way rather than how do you identify abuse in a reliable way. That latter part requires policy, trust, et cetera.

There are -- this industry has been around for 10, 15 years, has developed extremely reliable methods of identifying things that are being abused on a systemic basis.

Those things are then pumped into things like Internet Explorer, Google Safe Browsing, if you're using an email service like Gmail or Hotmail or something like that. These are all automatically put into these things today at scale in the millions on an automated basis within seconds of identification.

So the identification part, the technology, is highly reliable. There have been a lot of ways figured out how to white list things and reduce false positives to near zero. So the technology exists.

What -- the key is actually transforming those -- that information into action. And that takes contracts. It takes trust. It takes a whole bunch of things that have to be set up as a framework around that for people to take action in various venues, whether that's a domain registry, a domain registrar, an email provider, or somebody providing Web software.

So just wanted to answer that from a "it's a solved problem from a technology perspective." It's not a solved problem from a policy perspective necessarily. Thanks.

IRANGA KAHANGAMA: Thanks, Rod.

Can we go to the mic now?

DAVE PISCITELLO: Dave Piscitello from ICANN. I don't like the phrase "obvious abuser." It is certainly not what we measure with DAAR. What we measure with DAAR are the security threats based on blocklists, reputation lists, and, thus, what we perceive as abuse. And I think that's distinctly different from the obligation that a registry or a registrar or a DNS-hosting company or an ISP would have to go and take a look at what has been presented to them and do an investigation and corroborate the claim.

If I were in that position, I would be going and attempting to get the email that -- you know, that contained the URL, get the attachment that contained the URL, go to the site, do a WebGet or a curl, something that was benign. There are lots of procedures that one expects as due diligence on the registrar-registry level. And I'm not saying that comes at a zero cost.

But DAAR is not meant to be some place where you can go and you get the entire answer. DAAR is meant to be a mechanism to do a census of the entire namespace, the entire abuse threat landscape, and try to come up with some numbers that help us identify where policy is being successful, where policy may be lacking and how to create a synthesis.

CATHRIN BAUER-BULST: Thank you, Dave.

Graeme, let me throw this to the registrar. We've now talked a bit to the point of the range of different indicators that we have. So we have DAAR that provides a basis for an assessment, and then we've heard that there's more that needs to be done the registry and registrar side to turn that information into actionable tools to take action against possible clients that are not complying with your terms and conditions.

Now, that, of course, turns the focus on to those terms and conditions and on to what you need to be able to take action under those and how you can maybe also influence that in terms of how you set your policy. Could I maybe ask you to speak to that a little bit?

GRAEME BUNTON: Sure. Thank you, Cathrin. This is Graeme Bunton from Tucows.

There's a couple of pieces in there that I think are interesting, although Alan raised a good point. As you just said, linking, you know, the blocklist to actual evidence that is actionable, is nontrivial.

And I think to Dave's point what he was just saying is that -- you know, the methods that you can use to combat abuse on your platform, that sort of presupposes a certain level of sophistication on your sort of front line abuse queue monitoring staff that is frankly not available to all the registrars on the planet. Certainly, when you're optimizing for throughput to reduce your abuse queue, it's not necessarily something that you have a lot of time to go and dig into.

There's one other point I wanted to make because I hear it come up a bit. We've seen algorithmically generated domain names used for network management. So they're not always evil. There are a couple of places where people are using those for operating their businesses.

It is exceptionally difficult to track repeated bad actors based on what's coming into your abuse queues and how you monitor that.

There is no simple answer that we've certainly come up with, and it would be something that we would be very interested in because it reduces abuse on our platform, which is something we are very interested in doing. But it requires a very broad-level view of what's coming into your abuse queues that is not easily achieved.

CATHRIN BAUER-BULST: Thank you, Graeme. I think Alan also wanted to weigh in.

ALAN WOODS: Alan Woods again. I actually just wanted to say what Dave -- Dave Piscitello had said earlier, I just wanted to say if he was closer to me, I would have stood up and shook his hand because that was one of my -- a very important point to get across. And that is, DAAR is a project that shows statistics but work needs to be done in between DAAR and actual action by either a registrar or registry or another appropriate party. So, thank you, Dave.

IRANGA KAHANGAMA: Thanks, Alan.

To just quickly move into a little bit more specificity, Rod, you had mentioned that a lot of this has kind of already been done. Can you maybe talk a little bit more specifically about what type of data is needed to really enable these types of actions?

ROD RASMUSSEN: Sure. There are a wide variety of methodologies. It depends on the type of abuse, of course. So things that are really easy to detect are things that are generated by domain generation algorithms to give you one example. A domain generation algorithm is something used by malware to create a series of domain names which may potentially be registered in the future. If you reverse engineer the malware, you get the list of domains that are going to be potentially used. You can then watch for registrations of those domains and act appropriately because it may be a security researcher string rather than a bad guy. So that's one way.

Spam is an obvious way that's been done for ten plus years, 15-plus, 20-plus years probably as far as basic rudimentary analysis. It is very sophisticated now how you analyze that.

Various platforms, Facebook, the social networks all use these. The email program -- or email platforms all are looking at content when allowed by the users to take a look at things that are being done in a very large fashion and then taking a look at those domains, if it happens to be domains they're looking for.

From that, you will probably do something with that information to correlate maybe against some metadata that you might get from, say, a WHOIS query or a DNS query or looking into your own database of known or unknown objects. There are a whole series of formulas you can use to do that.

And then there are tools that are adjuncts to web browsers, there are network security devices that take a look at incoming and outgoing data flows on networks and correlate -- there are very sophisticated machine learning algorithms to find things like tunneling and other kinds of activities beaconing and monitoring on your networks. There's a whole wide range of technologies that can be brought together to form lists of those different types of abusive areas.

IRANGA KAHANGAMA: Thanks. I feel like you can talk about that all day. I guess one things that became clear is diversity of available data is really key in this field. T I think we have one remote question. We're going to be taking a remote questions later on that should be addressed. Cathrin, you want to ask the next question?

CATHRIN BAUER-BULST: Yes. I'd actually like to come back to this -- to the different types of data that we need to inform policy making, which Drew has very eloquently spoken to, this idea of seeing the general trends and developments that can inform policy making and from that to the more specific information that registries and registrars need to see to be able to take individual action in an individual case, which might require a different standard of evidence. It's not quite up to, of course, the criminal investigation or the like. It's something that, of course, can also be influenced by the terms and conditions of a given provider.

I just wanted to maybe come to Denise and your specific experience in also setting standards for communities and setting standards for customers. Is there, in your experience, lessons to learn from how terms and conditions can be drafted to enable efficient and effective reaction to abuse?

DENISE MICHEL: This is Denise.

So we have an extensive global system of security and abuse mitigation on all of our platforms that is continually monitored and updated.

And we coordinate broadly across the industries and sectors to share best practices, both in terms of terms of service but as well as data sharing for security as well.

I think the -- in looking at, perhaps, the contrast between what we do and what is done in some of the registrar and registry arenas, an element that hasn't really been addressed yet is incentives and will to do it.

The business constituency filed extensive comments regarding the abuse study that the CCT review did and offered some very specific ways that this study can be used as a stepping off point to increase our ability to collectively mitigate abuse and improve our efforts overall. Things like linking incentives to good practices for abuse handling, looking at fees that registries and registrars have to pay and linking those to best practices and results, making sure that we -- that this is the first abuse study and that we do this on an ongoing basis and can have rigorous and trend data that is actionable, that we increase compliance scrutiny on registries with high abuse rates.

There's a number of things that can be done right now to make this abuse actionable. And the sooner that we can get the open data initiative up and running and in the open domain and as soon as we see the DAAR report in beta form up on the Web site, the sooner we can do this. Thanks.

CATHRIN BAUER-BULST: We'll go to the floor. Number one.

REG LEVY: Thanks. This is Reg Levy from Tucows and ENOM. I'd like to address something that somebody said recently about terms and conditions. It's extremely true that most of us have terms and conditions that say we can take stuff down for any reason or no reason on our whim alone. But those are there to protect us, and they're not there to police the Internet or to do any type of monitoring. They're there in the event that there's something that we haven't decided before that is absolutely necessary in the moment and in that instance we have the legal right to do something. It's not there to just actually enforce our whim.

CATHRIN BAUER-BULST: In terms of -- I think we're going to move on to the next section in a minute. But I want to ask one last question to Jonathan on one point that has come up in the presentations on this idea of certain indicators.

So Drew said there are specific types of abuse that we look for, and then there's several vehicles. And he identified spam as one of them. And another one that he saw was that sometimes intellectual property infringements can be associated with abuse or can be indicators of likely abuse. Is there -- can you speak to those indicators and their usefulness in terms of helping to identify abuse?

JONATHAN MATKOWSKY: Sure. This is Jonathan Matkowsky from RiskIQ with the IPCM speaking individually in my own capacity.

First, in terms of a registrar's obligations under the registry agreement to -- under the registrar accreditation agreement to respond to abuse complaints and appropriately investigate them, this is a benefit for the community. So I would encourage everyone to take advantage of that and to use that opportunity to make sure that the community is protected from abuse. And this includes all illegal activity.

We can agree phishing -- the lull of phishing that steals your personal information is very much content-related.

We heard about how the SADAG report talked about typosquatted domains being used maliciously. And this is true in many different ways that IP -- and content is related to threats, to security threats. You know, especially complex threats where there's more than one Internet presence location.

And I'm sure everyone has read about in the news how Adobe Flash pop-ups have been used to lull people into downloading malware or that steals your CPUs on your computer.

So there's a definite relationship. And I would also say that the registry operators don't always have visibility into the registrars that are not responsive to abuse complaints. So they need to be notified when a registrar's not -- is not meeting its obligations so that they can take action.

This information would be included in the technical, statistical analysis, the data set that gets reported to ICANN. And ICANN can request it at any time.

So I would say that the DAAR study, the DAAR project should be used internally. I would encourage ICANN compliance to use it internally for ad hoc auditing. If you look back at the -- some of the data sets that I saw at least in the SADAG report, you can see how, even though there are fewer compliance reports filed, relatively speaking, against the volume of abuse complaints -- you know, Nanjing is there and so are others.

Look at Dynamic Dolphins, for instance, and see what happened. Just look on ICANN and see what happened in 2013.

So, thanks.

IRANGA KAHANGAMA: Thanks, Jonathan. I'm going to move the conversation along to the next slide. Thanks. Just as a reminder, how to create effective and transparent abuse reporting.

I think our first question I'm going to go to Tatiana to talk about David Conrad's presentation, which mentioned a number of different instances in which these blocklists were used in different Internet browsers and email that, you know, that, ultimately, non-commercial users, you know, also used.

And so I guess my question to you is where do end user interests overlap with some of these statistical analysis? And can DNS abuse data be effectively used and leveraged to create some sort of user-friendly tool that can inform the public of risks and potential abuse points online?

Tatiana?

TATIANA TROPINA: Thank you very much. Tatiana Tropina speaking.

First of all, I want to solve one confusion. I don't think that we are representing end users. We're representing non-commercial users, and there is a big difference because they can be both commercial and non-commercial.

But what I want to say is that we do have position on the entire abuse reporting tools and abuse reporting system issue.

I want to highlight again that we are NCUC. So we're not really collecting statistics, you know? We're not suspending Web sites. But what we stand for -- whatever tool is going to be used?

In my personal capacity, I can definitely say that I am for collecting statistics. I am for shared information and informing industry.

But here at ICANN we stand for clear line between technical side of DNS abuse being an ICANN mission and abuse solely related to a content. Because not everything that is illegal under applicable law would be a DNS technical abuse.

And we believe that ICANN and the tools used by ICANN should be related to the ICANN mission. I know that someone can bring their RAA here. But RAA is from 2013, and we have ICANN mission set during the transition period. So I believe that this is superior here.

Then, secondly, we have to be careful. I shared a lot about preventive approaches. Where the line of acting, reacting, and preemptive strikes here. So what does it mean to prevent? When is -- when are the players in the industry having to take actions? You know? What does prevention mean? And I think we have to be clear here. I told already that we have to have a narrow definition of the DNS abuse. And, as non-commercial users, we also believe that we should not forget that the main thing when it comes to abuse is not only to suspend Web site, but it is to catch those who are violating the law and who is actually abusing. And this is the work of law enforcement. Sorry. We'll take another 20 seconds.

So we do not want intermediaries or industry to act as a content police or as the police in any sense.

That's why we are getting scared when we hear the phrases that industry should police themselves. It should not. They should deal with DNS abuse anyway. Thank you.

CATHRIN BAUER-BULST: Thank you, Tatiana.

I'll just go to Drew next and see whether you have views from a security researcher point of view as to how frequently this data should be published to be useful. Is there any sort of minimum or ideal frequency that you would see for it to be useful to the security community?

DREW BAGLEY: Thank you. I guess, if we're looking at the study that I was referencing earlier that the CCT commissioned, I think it's very important that this is not something that merely comes out every five years, every time there is a review team looking into this issue or, for example, you know, other review teams, since I know this overlaps between multiple review teams. Instead, I think that, you know, either maybe to the extent DAAR produces transparent statistics for the community, it might be that just having this as an ongoing data set in some form would be very useful. And then with that what you would do is you would do periodic analyses of what that data actually means. So you have the data available to the community to slice up and analyze. And then maybe there are comprehensive analyses such as what the CCT's commissioned study did. Perhaps twice a year, I think that would be very helpful.

Because what it's very important for is to understand where the trends are, to take a long-view approach. Because certain phishing campaigns and other sorts of malicious campaigns can skew results in specific quarters. So it's very important to have an ongoing continual assessment so see where we are as a community.

If you don't mind, I would love to just respond a little bit to Tatiana's remarks. Because I think Tatiana made some terrific remarks that are really reflective of the diversity of the community and the viewpoints on this topic.

And that's why I think it's very important what I emphasized in one of my first slides is that instead of, you know, spending years going back and forth debating all the different things that could be abusive in one country but not in another and what not, it's very important we, as a community, start by tackling the things for which there is consensus and for which we actually already have authority through the form of the prohibited behaviors in the agreements and start with these very technical things instead of, you know, really getting lost in the weeds.

So I really think that it's important that we build upon what Tatiana said with regard to that. And I also think Alan brought up such a good point about how difficult it is if we're looking at things on the reactive side and actually looking at going after the abusers themselves. Because, obviously, that requires evidence.

And then, as Tatiana pointed out, a provider is not law enforcement. So there's different degrees between suspending someone for violating terms of service and then doing something about the potential criminal side of things.

That's why I really think it's important we shift to a proactive model where we are using obvious indicators to maybe wait until a domain goes live if there's something suspicious in the registration itself. Maybe it doesn't go live within five minutes. Maybe you have a manual review and it takes 24 hours before you allow a domain to go on or what not. I mean, there's going to be different models that work for different providers, but I think it's very important we shift to that model.

IRANGA KAHANGAMA: Thanks, Drew.

Dave, did you have follow-up?

DAVID CONRAD: Yeah. Just current plans relating to the publication that we're generating within the DAAR system is to generate a monthly report that, basically, documents the statistics that we're seeing at an aggregate level per registry, registrar.

And that information would then be -- then the plan is to actually make that data available via the Open Data Initiative over time so that people can do historical trend analysis and time series analysis based on the data that we're collecting.

But that's sort of the tentative plan. And we're actually very interested in any input the community might have about frequency of the releases of the data or, you know, the methodology by which that data is released.

IRANGA KAHANGAMA: Just -- sorry, really quickly, do you have also have a potential date to see the first report?

DAVID CONRAD: Right now we're actually doing sort of an evaluation of the licensing requirements that we have with the various data feeds that we're providing or that we're receiving.

So I'm not really comfortable giving a particular date. Because...lawyers.

[Laughter]

IRANGA KAHANGAMA: Fair enough. We can go to the mics now. Number 3, please.

MILTON MUELLER: I'm Milton Mueller at Georgia Tech. There seem to be two different approaches when we talk about DAAR. When I hear David talk about it, I hear we're collecting a bunch of data; we're issuing reports; and then those reports can be used to guide policy. But I heard the registrars and registries making the point that there's a lot of work that needs to be done intervening between looking at that data and taking an action.

On the other hand, I hear some talk about more preemptive actions that the data might actually guide certain kinds of preemptive actions.

So, in that regard, I have kind of a question about what DAAR is or is going to be. So how extensible would it be, David? The threats change. You're relying now completely on third party RBLs. You don't actually generate it? ICANN doesn't actually collect the data that those things are based on. You're simply compiling and making it a resource for the DNS industry, which I think is great.

But the threats change. The criminals change. Their techniques change.

And how will you respond to those innovations going forward? Are you developing a capacity to do that, or are you simply going to continue to rely on third party entities to get that data?

DAVID CONRAD: So the simple answer is we do what the community tells us to do.

If, in the context of DAAR, the threats that are identified that we track are the ones that were identified in the Beijing GAC communique. If, at some point, the community suggests that we track some other form of abuse, then we will see what we can do to incorporate that within the DAAR framework. It is extensible.

With regards to the data sources, the primary requirement for the data sources that we're using are that they be publicly available. If, for example, there is a data source that ICANN generates that we make available the ODI or some other mechanism, then we could potentially incorporate that into the DAAR system. But that, again, would depend on what the community demands are.

And I think my colleague, Mr. Piscitello, may have some input on this particular topic as well.

DAVE PISCITELLO: Yeah, a little bit. So I'm really glad you asked that question because there are a couple of things that I believe that we will be able to do in a year that we have never been able to do in this industry. We will have a year and a half of history. One of the things you can do with a year and a half of history is you can look at flocking and migration behavior. You can look at the delay or timing between a sudden spike in registrations at a given registry or registrar and how those names were used. So I can show you a graph, if I were able to show you a graph, that shows that there was a spike in a particular registrar of about a thousand registrations and then those registrations were actually given out over time after a curation period. Now, this is very different from some of the -- some of the measurements that the SADAG based their analysis of compromise versus maliciously registered domains. So that gives us something new to take a look at.

With respect to evolving threats, you know, I've had discussions with the folks that -- that are developing the system talking about adding boot or blacklists. Boot or blacklists are lists for distributed denial of service as a service site. That's an emerging threat. If we feel that -- that the data in that database is credible, reliable, accurate, public, all the criteria that we have, then we have to sit down and think, is this something we want to inject into our system because it benefits the community to know that this is another threat. But again, as David saved said, you know, we -- we've built a platform that is, I think, very, very extensible in many, many dimensions, and so long as we -- we understand what threats we want to measure and what we're going to use with the measurements, I think we can do a lot of what you're suggesting.

DAVID CONRAD: Thanks, Dave. I believe we have two remote questions. If I could get both of them read out and we'll address them, and then I think we're going to move on to the final third of three discussion points.

JAMES COLE: We have a question from Maxim Alzoba from FAITID. "Does ICANN's CTO office have plans, have interactions related to the DAAR tool with RySG and RrSG part of the community so the resource could be made useful for registries and registrars?"

IRANGA KAHANGAMA: Can you just read the second one, too. Sorry.

JAMES COLE: The second point is, "What is the reason to use a company with questionable practices, Spamhaus, as a trusted source? The escalation procedure of the company includes cutting up registrants and registrars, Internet, blocking mail servers of the registrar SAR system DNS servers with no accountability and no transparency to the community."

DAVID CONRAD: So thank you for those questions. You know, taking the last question first, the -- the use of Spamhaus is because within the anti-abuse communities Spamhaus is considered a -- a trusted and reliable source and had met all the criteria that we had specified in the initial sort of straw man construction of the selection for blocklists. It's also worth noting that regardless of, you know, what we may feel about a particular blocklist, the reality is that these blocklists are used by industry, by academia, by commercial and non-commercial providers to impact how traffic flows over the Internet and, you know, pretending that a particular blocklist is unimportant because you don't happen to agree with their policies doesn't change the fact that other folks are relying on that blocklist to block traffic from particular domains or IP addresses. If the criteria changes such that Spamhaus is not considered a viable alternative or viable contributor to our data, then obviously we can adjust things as necessary. And, you know, if there is demonstrable evidence that they're not living up to their own specifications about how they handle a request, then that's another area that we can look at. Our experience has been that the -- in many cases the folks who are -- who complain about particular blocklists is because they have been placed on this blocklist for one reason or another and have had challenges removing themselves. Any time we have evidence that a blocklist isn't doing what they say they will do, then that would serve as a reason for us to reconsider including them in the data feeds that we receive.

With regards to providing the data to the community, as mentioned our -- our current plan is to make that data available via the open data initiative. Currently on our plan is a monthly basis, but that's at the community's request. We can adjust that. Likely we can adjust that to meet whatever the needs are.

IRANGA KAHANGAMA: Thanks, David. I believe there's one more remote question that we have missed. I just want to go back to that very quickly.

JAMES COLE: This question comes from Kristina Rosette from Amazon registry. "What mechanisms and processes does ICANN intend to implement to avoid false positives and potential liability before making DAAR data publicly available?"

DAVID CONRAD: Guess that's me again. So as mentioned, we're not generating this data ourselves. We are relying on external parties to which anyone can subscribe, either via pay for license or openly available. If a report is considered a -- you know, is a false positive, that is impacting how these millions of users of these RBLs are going to be interacting with the resource, whether it be a domain name or an IP address. It's true that there have been false positives. There are frequently anecdotal descriptions of egregious cases of false positives. But the reality that we look at is the -- the -- and the criteria by which we select a blocklist is that they are vetted by industry and academia, that they do have documented processes by which names are added and removed, they abide by those processes, and that there is a clear mechanism by which those blocklists operate.

You know, with regard to questions about liability, I am not a lawyer and I will not play one on the Internet.

CATHRIN BAUER-BULST: Thank you very much, David. That will move us to the third part of our discussion. So we want to look in these last 12 to 15 minutes at how abuse reporting could support registries and registrars in their prevention and mitigation efforts? How it could possibly be used in contractual compliance and enforcement and how it could be used in policymaking." So we have already touched upon some of these issues. What we haven't talked very much about yet is how it would be used possibly internally within ICANN, and maybe I can throw a question to Jamie as to whether you have been also inputting your needs into this process and how you see this possibly being used by compliance in the future.

JAMIE HEDLUND: Thanks. I never hesitate to articulate my needs. But we -- we've been working closely with OCTO and the contractual compliance department, I think, is generally pretty excited about DAAR, for a number of reasons. One is it does help provide data-driven evidence focus for where we should deploy our resources. Secondly, if it's true that these lists that make up DAAR are used by businesses enterprises, others, to make decisions on email services and web access, things like that, then that should make our job that much easier because there should be a built-in incentive for those registries or registrars who may find themselves higher up in the -- in the hierarchy.

Just to be clear, though, you know, the output that DAAR is going to exhibit is at the aggregate level, as David explained. And that is not -- the aggregate level is not something we can use for contractual compliance. We have to look below that to find actionable -- actual evidence that can be used hopefully to -- to clean up some of these registries and registrars zones.

The -- the last thing I will say is that the -- you know, the outputs that I've seen have -- shows that there is a very, very small handful of contracted parties who are responsible for a very, very large majority of the abuse levels that it shows. So -- and frequently these are not the entities that are -- at least that I've ever seen active participation -- participants at ICANN. So I think if we can -- if we can use that data and make progress, not only is it going to be, you know, good for users and the Internet generally, I think it will also be good for the credibility and legitimacy of ICANN and the multistakeholder model which, you know, post-transition is a really important thing to focus on.

IRANGA KAHANGAMA: Thanks, Jamie. Oh, Alan. Go ahead.

ALAN WOODS: Just want to very quickly say thank you to Jamie for that. It is good to hear. What I just also want to point out is it is a true point about those bad actors out there and that, you know, there's an awful lot of registries out there who are really, really trying their best in order to do this and proactively engaging and showing up, you know, at ICANN meetings and having these discussions. I mean, from my point of view, from Donuts, we are all for enforcement. Once we get that evidence and that done and be able to decide and be able to test evidence in that way, then absolutely. I mean, we would be more than happy with that.

IRANGA KAHANGAMA: Thanks. Graeme, did you raise your head? No.

GRAEME BUNTON: Sorry. No, sort of. This is Graeme for the transcript. You know, registrars are very much in favor of removing the bad actors from the platform. It reduces the burden that we find on the rest of us who are working very hard to keep our platforms clean. And it reduces a lot of the policy implications, too, as we're striving for policy solutions that are going to apply to all contracted parties or all registrars when really the solution should be quite targeted and narrow because it's a specific actor. And getting to that place, I think, solves a lot of problems and makes all of our lives a lot easier. Thank you.

IRANGA KAHANGAMA: Microphone number one.

GREG MOUNIER: Hi, everyone. Greg Mounier from Europol. I've got a question to Graeme and Alan. The domain name industry's a profit-driven industry and it seems to me that proactive NTWS (phonetic) measures often seen by the industry as additional cost. So my question would be, how can -- what would it take to actually turn the logic around and make sure that proactive NTWS measures are seen by the industry as a competitive advantage. So in other words, when are we going to see, for instance, in the marketing strategy of Tucows to say at Tucows we have the lowest rate of abuse therefore, you're safe with us and therefore, you make more money.

[Applause]

GRAEME BUNTON: Thank you, Greg. This is Graeme, for the transcript. That's a good question. I'm not sure. I think being proactive also introduces some liability that also we have to take into account when we're looking at our bottom line as well. And so the technology just needs to get to a place where we can be proactive about our registration in a way that I don't think it's there yet, or at least I haven't personally seen it demonstrated.

IRANGA KAHANGAMA: Rod, you have a follow-up?

ALAN WOODS: Just Alan Woods here as well. Donuts as well. I mean, we take it very seriously. And, I mean, that's part and parcel of the way we approach DNS abuse as it is. But, I mean, we're members of things like the DNA and the healthy domains initiative and trying to do the industry initiatives, the voluntary initiatives, those ones that put us and set us apart as, you know, a good actor. And again, doing that.

Also, you know, ever time we take down a domain as well, it does, in effect, teach the abuser to go somewhere else as well. And that's another issue that we need to think about. We can push them away from our platform, but they'll just find another platform, one of the bad actors. So we do need to focus on getting rid of the bad actors as well.

IRANGA KAHANGAMA: Thanks. I want to -- (saying name) is in the queue so I want to give him a chance to speak.

ROD RASMUSSEN: Thanks. Rod Rasmussen again. So this is -- this very first point on the discussion here is why I came to my first ICANN meeting. I was representing the anti-abuse industry and trying to have a discussion with registrars. Unfortunately, that was the Vancouver meeting and some other things happened that meeting that kind of got in the way of making this a big discussion. You can look up the history. Anyways, my point being is that -- and that was well over ten years ago. And a lot of this has been done and has been done successfully. There are plenty of examples. One example is that the anti-phishing working group, myself, and many of you know Greg Aaron produce a regular report, and we've been doing it now since 2007, on trends in domain registrations used for phishing. Those reports have been used in conjunction with registries and registrars to identify problems and trends and have changed their policies as to how they deal with things. And that's both in the ICANN space and the ccTLD space. In particular ccTLDs have had some major issues and been able to clean them up as a result of looking through patterns and figuring that out.

Further, a lot of registries and registrars have set up various reporting mechanisms, automated reporting mechanisms, with various kinds of back-end frameworks. One of those frameworks would be contracts. So in my previous life, I had a company that had contracts with those kinds of entities to be their agent to figure out whether something was abusive enough or not and make a determination on their behalf and take that down. Another one is a trusted intervener program where you are actually accredited and are able to then again move that trust to someone else who actually has that expertise in order to be able to do that. So again, you can automate and move these things, and the models do exist. It's more a matter of getting that information out so people can use them. Thank you.

CATHRIN BAUER-BULST: Perfect timing, Rod. So we have mic number one.

DAVID TAYLOR: Thank you. I'm David Taylor from Hogan Lovells. I'm a lawyer so you can all boo it, but I'm also on the CCT review team so you should all cheer, I think. Which means I'm with that guy with the beard. The question I have really is, on the abuse reporting and that it's something which is obviously a key issue and there's a lot of good registrars and there's a lot of bad registrars. There's a lot of good registries, and there's some bad registries. And we know when we go after people that it takes quite a lot of time for an individual registrar sometimes to take the domain name down, even when you've got very clear illegal abuse, and illegal activity. I mean very clear. It would easy win in a court of law. You can still be playing duck and dive for three to four weeks trying to get them to take it down. So we could go to ICANN compliance and in some instances we will.

But when you get a registrar, as Drew showed before that, when we have one that's been taken down -- and, Jamie, we talked about this one, but you mentioned the registrar AlpNames there -- that's such a high level of abuse when you see something like a .SCIENCE with 51% of the zone file being abusive domain names and you see it still up there and alive, and you see the registrar still not be accredited after, perhaps, one year or maybe six months. But for the layman, how -- why does it take so long to deal with an issue like that when it seems so evident? And obviously there's reasons, and don't go into the things you can't go into, but I still try and -- I fail to understand that, and I have difficulty explaining it to clients.

JAMIE HEDLUND: So it generally comes down to two things. One, actionable evidence and an aggregate report that any particular contracted party is -- has high levels of abuse is not enough. You need actual evidence that we can -- we can move on.

The second is there are some limitations in the contract itself. So we can't, on our own, order a domain suspended, for example, or taken -- or taken out.

And one thing that I think will -- that I'm hopeful will come out of using the DAAR output and the underlying -- some of the underlying names is it will show where we succeed and where we fail. And where we fail and there are persistent bad actors out there, despite our -- our efforts to use the tools that we have, then that's information that will go to the community for the community to use in their policy development.

And so even where we don't succeed in helping to clean up registry/registrar space, the community and people like yourself will have, you know, evidence of where that's not worked and hopefully be the source for information on -- or the source for change in policy or contracts.

IRANGA KAHANGAMA: Thanks, Jamie. Really quickly. So just a last comment before we wrap up. I want to let Denise weigh in as another affected party in all of the reporting and how that would be used in any decision-making.

DENISE MICHEL: Sure. So the -- The SADAG report, the CCT abuse report, showed that new gTLDs experienced a rate of abuse that was almost ten times higher than were experienced in legacy gTLDs. The abuse data provided in that report and related information is very useful and relevant to, for example, the rights protection mechanism PDP that's going on right now and subsequent procedures PDP that's going on right now that will create -- it's looking at creating policies for the next round of new gTLDs.

That's just one example. There are many others that apply to things like privacy/proxy implementation and other efforts within ICANN.

But it really comes down to having the abuse data and information and trends that can inform a whole host of activity within ICANN. We should be a community that uses real facts and data as an understanding, as a foundation for our policy-making. This is absolutely critical to do that. And if there's something we can do, David, to move the lawyers along, so we can get the DAAR report into the public sphere and we can get the ODI initiative and the data there started again, I think it's been stale for about four months, that would be really helpful. And we really look forward to supporting these efforts in the future.

Thanks.

DAVID CONRAD: Just for clarity. I was, of course, kidding about the lawyers blocking action here. We're having to go through just clearing the license agreements, and that takes a little time. We're very confident that we'll be able to move forward with some (indiscernible) statistic reports in the very near future, and the larger and more comprehensive information in sort of the form of a spreadsheet, you can imagine, should be coming soon after that.

CATHRIN BAUER-BULST: All right. Thank you, David. We're running up against the clock, so we're not going to be able to take any more questions. I apologize. I think what this debate has shown is there is more debate to be had. It has brought together some of the different perspectives on abuse mitigation, and I think it's been very good in terms of highlighting the different needs of various parts of the community, from policy-making to taking individual action, either on the preventive or on the reactive side, and it has helped identify ways in which data could be used and, hence, informs DAAR.

And I think one very interesting perspective that has come up in the interventions of David and Jamie notably is there's a very small handful of contracted parties where abuse is concentrated and that's where, from our perspective, the aggregate meets the specific, because of course there is action that could be taken. Even if there are two false positives out of the 76 examples that Drew has cited, then you would still have ample other data to take forward some form of action.

And what we might want to look at in the future is how we can narrow that gap between the aggregate and the actionable. And for this -- I think we might come back to this idea of the principles that Iranga talked about in the introduction, and I'll turn it over to him to continue that part.

IRANGA KAHANGAMA: Thanks.

I want to say thanks to all the panelists for participating. I think -- Yeah, I think it's important to move this conversation forward, and I guess I will proactively sign the PSWG up to kind of keep guiding this discussion along. But I think the community deserves a proper mechanism at the cross-community level to really organize and aggregate these issues to really move the ball forward. So I think we're going to go back and try and think of how best to move forward in addressing some of these issues and providing the right mechanism for the community to continue addressing DNS abuse mitigation efforts. And hopefully we can use this as a forum to kind of both keep the community abreast but also to keep the community transparent and open enough to move along and progress on this front.

So I want to thank everyone for coming and hopefully participating in future events like this.

Thanks.

[Applause]

[END OF TRANSCRIPTION]