COPENHAGEN – Cross-Community Session: Towards Effective DNS Abuse Mitigation: Prevention, Mitigation & Response
Monday, March 13, 2017 – 13:45 to 15:00 CET
ICANN58 | Copenhagen, Denmark

CATHRIN BAUER-BULST: Hi, everyone. We're going to start this session in a few minutes but in the meantime, can I already encourage you to come closer. Because this is explicitly not a panel. This is about talking to you. So come and be part of the conversation. There's lots of room up here, lots of microphones, so feel free to move a bit closer to us. Thank you.

All right. Good afternoon, everyone, and welcome into our session on a more effective approach to DNS abuse mitigation. My name is Cathrin Bauer-Bulst. I'm from the European Commission. I'm also one of the co-chairs of the GAC Public Safety Working Group. And I'm here today co-moderating with my colleague Bobby. Do you want to briefly introduce yourself.

BOBBY FLAIM: Sure. Bobby Flaim, Federal Bureau of Investigations and member of the Public Safety Working Group.

CATHRIN BAUER-BULST: Thank you. So why are we here today? So those of you who were in Hyderabad, you may remember we had a first hit session where we had a sort of stock-taking exercise on where we stand on DNS abuse mitigation, and with this session today we want to identify more concrete steps on what we can do to move towards that lofty goal of effective DNS abuse mitigation.

Now that, of course, brings us back to a more horizontal point that we've always discussed, but that's becoming more important, especially now after the IANA transition, the role of private parties in this ecosystem.

So as we all know as a general rule, private parties are not, per se, asked to enforce any laws. However, given the hybrid role of ICANN and this community, has made us all pour interests into a contract between two parties and that means that we have clauses in contracts like in the 2013 RAA and others that are included in the interest, not necessarily of the two contracting parties themselves but also of third parties who are not parties to that contract.

So how do we deal with this challenge and how do we ensure that the third parties, who are outside the contracted self, are part of the process in following through on contract clauses and how do we ensure transparency and accountability on all sides. That also explains why the GAC is interested in this topic and is

sponsoring this session, and Bobby will now provide us with a bit more background on the GAC involvement in this topic.

BOBBY FLAIM: Thank you, Cathrin. One of the things the Public Safety Working Group, with the endorsement of the GAC, is we came out with some GAC follow-up advice and some advice concerning DNS abuse mitigation and security, and particularly how the security department of ICANN and contractual compliance work together to kind of address abuse complaints that they have received independently or they've researched independently and what is done.

Specifically, we focused on three areas. The first area for GAC follow-up advice was the 2013 RAA, or Registrar Accreditation Agreement. So if you remember, there was GAC advice in 2010 concerning some of the provisions of the RAA such as WHOIS specification, duty to investigation, accreditation, vetting, and so on and so forth.

One of the things that we still wanted to follow-up which we haven't seen implemented was the cross field validation of addresses and the WHOIS specification. And some of the other things we wanted to explore insofar as GAC follow-up advice is to see if the 2013 RAA provisions are actually doing what they

intended to do. Is that enabling contract compliance to be more effective in mitigating abuse, what further can be done, so on and so forth. So that was the first part of the GAC advice which is in the Hyderabad communique known as annex 1.

The second part of annex 1 in the GAC communique from Hyderabad concerned the GAC safeguards, specifically the new gTLDs, and some of the things that were in there was how registries would address security issues. In particular how they would analyze them and how they would report that to ICANN. So again, we wanted to follow up on that GAC advice and see what the effectiveness of that advice was to see are there reports coming in and if they are, in fact, having that desired effect.

The last piece of the annex 1 which we were hoping to discuss further, that's why we have Maguy and Dave here, is to see what the relationship is within ICANN, to see how they address abuse. In so far as the security team, how they receive complaints, how they investigate complaints, what they do with it, and how that message is transported over to contract compliance and to see if that may be an effective model in so far as trying to mitigate abuse that way as well.

So those are just some of the things from the GAC perspective and the Public Safety Working Group perspective that we're hoping to discuss further here today.

CATHRIN BAUER-BULST: And to launch us into the presentations, the first one now will be by Greg Aaron from the Anti-Phishing Working Group. So over to you.

GREG AARON: Thank you, Cathrin. My name is Greg Aaron. I'm here today representing the Anti-Phishing Working Group where I am a senior research fellow. The APWG is one of the major industry associations dedicated to research, education, and helping public and private entities deal with Internet crime. Specifically phishing, but also malware and other forms of Internet identity theft. I'm also a professional cybercrime investigator. My full-time job is with iThreat Cyber Group and I'm also a member of the ICANN SSAC. Let's see if this clicker works. It does not. Please advance the slide.

Okay. This is information from the Anti-Phishing Working Group about the amount of phishing that it has recorded since 2009. And you will see that the red trend line is very persistently moving in the upward direction. 2016 was the first time in which

the APWG recorded more than one million phishing attacks during a year. And what we've seen is, you know, a steadily climb in the amount of phishing that's taking place and also the number of domain names that are involved.

Look at 2009, for example. Phishing that year doubled almost from the year before. And this is a good example of the kind of thing we're dealing with. That year a lot of this phishing was attributable to a gang which was called the Avalanche Gang, and they set up a large botnet and they did a tremendous amount of phishing that year. The next year they moved to doing malware. And so their activities disappear from this chart, but this group did this work from 2008 or so through 2016. And the ringleaders were arrested on November 30 of 2016. My point is that this is a group that was able to do their work over a very long period of time. In the recent years, for example, they're responsible for the theft of at least 6 million Euros just from German online banking, but they were hitting targets and victims throughout Europe and North America and elsewhere in the world. The total losses will probably in the end Europol thinks be in the hundreds of millions of Euros. Next slide, please.

Here's some of the realities of dealing with cybercrime and specifically cybercrime that involves the Domain Name System. As I mentioned, with the Avalanche Gang, a lot of this crime is

very professional. That group, for example, had this botnet, but they rented it out to other criminals. There are services that criminals use and sell to each other. They're very good at what they do. They're profit-oriented.

One of the things we also see is that abuse tends to concentrate in certain places in the domain name space over time and it moves from place to place over time. That means a lot of domain names that are being used may be registered at certain registrars or in certain TLDs. The activity is hosted at certain hosting providers. One of the questions is, of course, why does it happen in those places? Well, some of the answers are that criminals like to be in places where nobody's going to bother them, where they can continue their work as long as they can. So they like hosting providers, for example, that look the other way or are not paying attention to what's going on or who their customers are. And that is also true in the domain space as well. Sometimes it's due to inattention. Sometimes low price matters. They like low prices, as much as anybody else. It keeps them under the radar in some ways. There are also cases where criminals are operating infrastructure that they own and operate themselves for the purpose of crime. This happens in various kinds of services. But it also happens in the domain name space. We have had several registrars over the years that were owned

by criminals. Two of them I mentioned here, EstDomains and AB Systems. They were owned by criminals. They were eventually arrested for cybercrime and wire fraud and things like that. The registrar who owned AB Systems actually was also running guns in Asia and was actually putting out contracts on the lives of some of his former associates. Those people do exist.

A fact is that mitigation is usually not done in this space by law enforcement. Law enforcement is working under some constraints. They have limited resources. Each law enforcement agency can only work within its jurisdiction, and so it has to set up cooperation on particular cases with it's -- their colleagues in another jurisdiction. That takes time. Also, prosecutors do not want to take on cases that they absolutely know they cannot win.

So the international aspect of cybercrime, it really works against law enforcement in a lot of ways. Instead, what we're looking at is an environment in which private parties are trying to keep the lid on things. They're looking to protect their customers and themselves. And what they use are contracts. They leverage the contractual relationships. If you want to use a service, if you want to use Google or Facebook, for example, you're entering into a terms of service and you agree to abide by those terms of service. Those same contracts govern hosting

and everything else. And that's where -- where people are leveraging the contracts to get that activity shut down.

Unfortunately, criminals know how these things work. They understand the domain space and they do not play by our rules.

Next slide, please.

Here's an example of some reputation data from an organization called SURBL. Their data is probably being used to protect your mailbox and your browser. And on their website, this is information they publish. They list domain names that they consider to have bad reputations. Number one is .COM, but we would expect that. .COM has something like 148 million domains in it. It's the large largest TLD.

Number two is .TOP. .TOP is a much smaller domain and has about 4.6 million domains in it but it's number two here.

Number three is .SCIENCE. .SCIENCE only has about 250 or so -- 250,000 domains in it right now, which means that about half of that TLD is considered to be a problem, at least by this provider.

So we can see from some data where the problems are. And the question is why is it clustering in places like these? What's happening? Who is using these domains? Who sold them?

Next slide, please.

So from my perspective and the perspective of the security community, I think, we look at ICANN's role this way. ICANN does have a role to play in stability and resilience. There is a public interest. There is disagreement about exactly how far that extends and to how you can define that, but we are all interested in an Internet that is usable and safe for users.

ICANN is the one who is accrediting registrars and registries, and as part of that process, the community has had some input into what the contracts say. And some of the tools that we have to deal with problems include the WHOIS accuracy provisions. There are provisions in the contracts against using domain names for malicious purposes, and registries and registrars do have some responsibilities for monitoring what's going on, response, and reporting.

Those contracts exist because they are enforceable.

The question then becomes how does ICANN use those tools and enforce its contracts.

As I've mentioned, personally one of the things I think we have to concentrate on are using those tools to concentrate on the worst problems, because they -- they do cluster in certain areas. And as a security professional, I worry about repeated problems

in the same places. Things that happen over and over again at scale.

And when those things happen, are we looking at dealing with them and holding parties accountable if that is the right thing to do?

Thank you.

CATHRIN BAUER-BULST: Thank you very much, Greg.

So in terms of running the session, we're going to take a break after this presentation to now have a Q&A and discussion with you. And while you -- You can participate from the microphone up here in the front in the middle. We would ask you to please identify yourselves and -- yeah, and then state your question or statement.

And while we're waiting for people to possibly come up and participate, I was just wondering, in listening to you explain some of the difficulties that we see in terms of mitigating abuse and the Avalanche case in particular, are there practices that you saw as best practices in places where -- where there is effective abuse mitigation or in places where you do see

cooperation with law enforcement succeeding in combating abuse.

GREG AARON: What may not be visible to the community is that these kinds of mitigation activities take place every day. It's actually quite a regular occurrence. Registrars and registries receive information, sometimes through their own monitoring or sometimes through reports from other people, and domain names are suspended, hundreds to thousands of them, every day.

So in some respects, things can work very well. However, that requires all the parties to be communicating and requires them to be willing to do their part.

A lot of the problem is not with the parties who are here at the ICANN meetings. It's some of the parties who don't come to the ICANN meetings.

So there are a lot of successes. But like I -- the avalanche investigation took four years, and it was known before that that it was going on. And during that time, that group consumed at least a million domain names. That's a lot of domain names. And some of those were dealt with at the time, but they were also able to consume that number of domain names and

register them and always get more. So that indicates a repeatable problem.

CATHRIN BAUER-BULST: Thank you, Greg.

Now we'll open the floor for the first question. Please.

JIM PRENDERGAST: Sure. Greg, Jim Prendergast, Galway Strategy Group. I'll give you a real softball to warm you up.

I notice this presentation isn't on the meetings page. Can we get it posted there so we could look at it a little more closely? There were a lot of numbers that went by pretty quick.

CATHRIN BAUER-BULST: Sure.

SHANE TEWS: Hi. Shane Tews, (indiscernible). And actually, this is to Maguy. I was in your session earlier today. Greg had great analytics. And that's the one thing that I think we're all challenged by on compliance, is -- and I realize you have the challenge of trying to keep people's privacy but yet letting us know what the problem

is. Because like you were saying, Greg mentioned that these guys start and they're phishing and then they move to malware, but they're able to see it's the same group in a lot of times. So it's easier for law enforcement to track them.

Is there a way in your process that if someone -- like a check-the-box, if they don't want to make their information available, could you give them a screen name or you could do something that would allow us to follow? And we're really looking for trends. We're not looking for specifics on the individual cases, per se, as much as seeing is there a trend that people are following? Because that would allow, I know, law enforcement and the people that are looking at the cybersecurity side of the process to see is there a potential issue that somebody is complaining, and is it towards the contracted party house or is it outside of the scope of ICANN, that those would be the kinds of things that would be really helpful for us.

Thanks. David, if you have a thought on that, too.

MAGUY SERAD: Thank you for the question. So I'm going to start addressing it from the end forward.

SHANE TEWS: Okay.

MAGUY SERAD: There is a way to track what we call reporters or complaints, people who submit complaints to ICANN contractual compliance. And if there is an issue or concern that's been observed by the contracted party, whether it's an abuse of the system, we have the ability to review that and address it based on the evidence provided to us.

Now, coming at it from the front end of your question about the ability to have additional depth and details to the complaints that compliance receives, I think so that's one of the recommendations we hear from the CCTRT team is additional granularity.

So we are working with -- I've read the report a couple of times, and we'll be working with the CCTRT team and the team that's put together to better understand those requirements and work towards analyzing what will it take and how can we provide that level of granularity.

SHANE TEWS: That would be very helpful. Thank you.

MAGUY SERAD: Thank you.

CATHRIN BAUER-BULST: Thank you, Maguy.

I have Megan, and then the gentleman here at the front, and then we go back to the floor mic. Please.

MEGAN RICHARDS: Thanks. I have my own mic so I don't have to stand up, which is convenient.

It's Megan Richards. I'm the GAC representative for the European Commission, and I'm also on the CCTRT team, which is one of the questions I was going to ask, but I'll drop that one.

I wanted to ask you a question about your phishing list. You gave us the gross numbers, and of course what's important in that context is the relative importance, because in .COM, as you say, there are ten million registrants. In SCIENCE, only 300,000, whereas the numbers have a huger impact .SCIENCE than they do in .COM.

And I wondered, from your data, do you see a distinction between the ccTLDs, the new gTLDs, and the legacy TLDs? And somewhere Drew is in the background, and he is also looking at

this because the CCTRT team is looking at DNS abuse study as well. Bringing all this together will be very helpful also for the GAC in terms of the way in which it reacts to this and actions that can be taken either with national ccTLDs or in other context, too. Thanks.

GREG AARON: I'm currently working on a paper that will be published next month in cooperation with my research partner, Rod Rasmussen. And this will be an APWG paper. And we're going to detail all of the phishing that took place in 2015 and 2016 and do a breakdown by TLD and a number of other contracts. It's a large amount of data. We're hoping this is a definitive publication about the last two years, and we'll see exactly what happened where.

So that will be coming out next month, and that will include breakdowns by TLD and type of TLD.

CATHRIN BAUER-BULST: Thank you. We'll take the question here and then the four people who are currently there and then we will close the discussion for now but not to not continue it after the next presentation and the final ones.

Please go ahead.

UNKNOWN SPEAKER: I'm Sahir (phonetic). I'm going to translate.

Good evening. I would like to thank you for the information that has not been very promising and the presentation about the abuse in 2016 have gone into the millions, and that is a number that is not -- really doesn't make us very happy or very pleased. But in slide number two, I assume that the way to mitigate the abuses depends on the private sector more than the legal authorities. And as everybody knows, abuses, unfortunately, is not happening from amateurs but more from professionals. And I would like to know the opinion about the legal authorities having to take the lead and be the leading part in taking care of the abuses.

GREG AARON: Abuse moves quickly. In some cases criminals register domain names and use them the very same day. It's too fast for law enforcement to -- to try to take care of those things every day. They have to concentrate on certain cases over a long period of time.

So these are actually old problems. The private entities, the network operators and all the other service providers, have been dealing with these problems for years because they're the only ones who can do it.

I think a good discussion for here at ICANN is when we see these problems happening over and over again, what can we do about them? Is that something we want to concentrate on? And that involves the compliance department, for example.

Crime moves very fast. It's not something that legislation, and so forth, can deal with on a day-to-day basis down -- down at the ground.

CATHRIN BAUER-BULST: Thank you.

Can I ask speakers to please speak a bit more slowly for the translator, and at the same time, to be extremely concise so we can move on to the next presentation.

So you're the first to start this impossible task. Please.

WERNER STAUB: Thank you. My name is Werner Staub from CORE Association.

I would like to make reference to the list we have on the SUBL of TLDs that have an extremely high percentage of abuse. Two of those that I just saw were from a party that just won an independent review case against ICANN. So that speaks a lot about the amount of information that should flow between people working at ICANN.

If it is possible for a party that engages at least in complicity with that kind of abuse, and there's more details that are actually quite appalling, if you look at it in detail, that such a party is able to win a proceeding against ICANN.

CATHRIN BAUER-BULST: Thank you for that.

Do you want to react? Go ahead.

DENISE MICHEL: Denise Michel with Facebook.

Greg, I'd like to go back to your last point, and if you could expand upon your thoughts of whether the contractual -- current contractual obligations are being used effectively to address the large abuse trends that we're seeing in gTLDs. And if not, what suggestions you have for that.

GREG AARON: I think it's more of a -- that's probably more of a question for Maguy, but what I do see in my work is, for instance, registrants who own tens of thousands of domains, and they have faked their WHOIS information. So I know that they have -- there's something going on there. That's an indicator of bad faith on the part of the registrant. And then we can see what happens with those domain names.

And I do get concerned when I see those same things happening over and over again in certain places, yes.

DENISE MICHEL: Maguy, perhaps you could address that in your presentation.

UNKNOWN SPEAKER: Hi. (saying name) As the list that Greg showed, we also published a list very similar to that, outcomes very similar. The one thing we do do is we adjust for the size of the TLD and the size of the usage of certain number of domains and number of TLDs.

And also, to answer a question asked over there, we see a lot of difference between abuse being -- and ccTLD space versus the traditional gTLDs versus the new new gTLDs. There's quite a lot

of difference going on there. And it's very explainable why it happens, I think. But it's also a sign that I think there's a lot of room for improvement.

CATHRIN BAUER-BULST: Excuse me. Before you go away, can you tell us what the difference is? You see a difference, but you didn't tell us what the difference is.

UNKNOWN SPEAKER: The difference in amount of abuse. If you look at most of the traditional ccTLDs, they will have much stricter policy for domain, for example, you need to live in the actual country or you need to have an owner that lives in the country. Whereas, for some of the gTLDs, there's no entry at all. It's just open for everyone. I think that makes a large difference.

The other difference that is pricing. Domains that are cheap will attract abuse, because people who are in the business of doing abusive things they only care about one thing. That is a label in a DNS that lasts for a certain amount of time. After that they abandon it. They consider it a throwaway resource. If you're in the business of throwaway resources, you want it to be as cheap as possible.

DREW BAGLEY: Hi. Drew Bagley, the Secure Domain Foundation and CrowdStrike.

As Megan mentioned, I'm on the CCT review team. I just wanted to give a plug for our DNS abuse study in the hopes that we could get more data feed. So tomorrow at 11:00 there will be a session detailing the comprehensive DNS abuse study that's being carried out by SIDN and TU Deflt that will take a look at abuse in the new gTLDs versus the legacy gTLDs over a multi-year span. I know the vendor wants to try to use as many data feeds as possible. So, to the extent that anyone in this room can contribute data feeds or know someone who can or to the extent someone can comment on the methodology tomorrow, that would be much appreciated. Please show up. Thank you.

CATHRIN BAUER-BULST: Thank you, Drew. We really look forward to seeing that report.

We're going to close the questions here. Before turning to the next presentation, let me just remind everyone that in the Adobe room, we also have the scribe feed available. So if ever you need translation or you want to read along, it's also available in the Adobe Connect room.

BOBBY FLAIM: Can we just ask you to hold your question just until the next presenter? We want to get to everyone, but we see we're kind of getting short on time. So what we're going to do is the presenters will present for five minutes. And we'll have just about another 5 or 10 minutes for questions for that specific presenter.

And then we have allotted time at the end for general session questions. So, if we can do that, that would be fantastic.

Thank you, Greg, for your presentation. I think it was very good. Because we explored the ways in which we're seeing lots of abuse and trends and what would be a more effective way to maybe work with ICANN and Dave to see how we can marry those trends and how, on an enterprise level, we can be a bit more effective.

I just want to take the opportunity to introduce our next session speaker. His name is Craig Schwartz, and he's the co-founder of the Verified TLD Consortium. But he also is the registry for .BANK.

So, Craig, if you're there, can you go ahead.

CRAIG SCHWARTZ: I'm here, Bobby. Can you hear me all right?

BOBBY FLAIM: Yes. We can hear you fine. Thank you.

CRAIG SCHWARTZ: Terrific.

So fTLD Registry Services is pleased to participate in this session today and to share our experience operating the .BANK and .INSURANCE top-level domains, two of the most restrictive and secure commercially available TLDs today. It's our registration restrictions and mandated security that mitigate, if not all together eliminate some of the abuse topics that you're discussing today.

I'm actually trying to get the slides to coincide with my presentation.

BOBBY FLAIM: Craig, if you can let us know when you want us to switch slides.

CRAIG SCHWARTZ: If you can just move through my deck, that would be great.

BOBBY FLAIM: Okay.

Craig, we may be having some troubles displaying your slides. So, if you want to continue to talk through your slides, we'll try to get them up in the meantime.

CRAIG SCHWARTZ: Happy to do that. So there's a lot of detail in the presentation today. And I'm here to offer some highlights and primarily to answer questions you may have.

As the registry operator, we've gone to great lengths and significant expense to develop policies and procedures and requirements for our domains that are designed to serve and protect global banking and the insurance communities and the consumers they respectively serve. As the one-time community applicant for our TLDs, all policies and requirements were developed by representatives from the global financial services community as well as those from registries, registrars, and other subject matter experts in areas such as security and DNS operations.

The integrity of .BANK and .INSURANCE is preserved first by our policies. That is, strictly defined eligibility standards, which is the who can get a domain name in .BANK and .INSURANCE, a name selection policy to ensure that domains only get in the

hands of registrants that can demonstrate a right to them. That's the what a domain -- a registrant can have, an acceptable use and anti-abuse policy that extends to how domains may be used beyond the typical anti-malware anti-spam references you typically see in these types of policies.

And, secondly, by registrant verification prior to domain award. We'll get into more details on the next slide.

Security requirements were developed by a community-based working group which are actively monitored. And we send compliance notices weekly to all registrars and registrants about infractions we notice.

And we do have a prohibition against privacy and proxy services so that bad actors cannot hide should one get into .BANK and .INSURANCE. And to date we're not aware of that ever happening.

Regarding registrant verification -- and this has been a core part of our TLDs from when we were an applicant now to being a registry operator. We always planned to do this verification prior to domain name award to ensure only eligible entities are permitted to register domain names they have a right to. We knew it could be done, and we also knew that it would be one of the biggest expenses we would incur operating our TLDs.

With respect to selecting a verification services provider, in 2014 we issued a request for proposal. We got a number of submissions. And we ultimately chose Symantec, a global leader in security in verifying the authenticity of organizations, to be our service provider.

When Bobby and I were talking about this session a little bit earlier in the week, he did ask if we could share some cost-related information for verification. And what I can tell you and what I will share is that proposals for verification services came in at anywhere between 80 U.S. dollars and 104 U.S. dollars per registrant and sometimes with an additional small per domain fee.

In addition to registrant verification, we also have a number of mandated security requirements such as DNSSEC, in-zone name server requirements, specific encryption, and also that email authentication be used. These are detailed in great levels within the information on our Web sites.

As noted earlier, fTLD practically monitors for compliance with all of our technical security requirements. And this, too, comes at a significant operational expense for us.

Moving on to some of the operational highlights -- registration restrictions and verification coupled with security are essential

for .BANK and .INSURANCE given the public trust implications for these domains. And I would suggest that there are other TLDs that fall into the same bucket.

I'm also pleased to share that, in almost two years of operations, we've had zero cases of reported abuse using a .BANK or .INSURANCE domain name.

I'd also like to share that we've gone to pretty considerable expense to develop a number of resources to help registrants understand the value proposition of our TLDs and to help them activate their domain names.

And, sure, it's certainly good to sell a lot of domain names. And across .BANK and .INSURANCE we have about 6,000 registrations to date. But, if registrants aren't actually using their domains, what's the real value?

Actually, before I get to the gTLDs, let me come back to one other item. Since I mentioned that operational expenses are high for fTLD registry services, you may be interested in knowing that our domain names generally retail for about a thousand to 1500 U.S. dollars per domain per year, depending on what registrar or registrant uses and what types of services registrants purchase from them.

I do want to make a plug, as Bobby noted in the beginning, that fTLD registry services is a cofounder of the Verified Top-level Domains Consortium. We're a group of like-minded registries, including .PHARMACY, .NET, .REALTOR, who are advocates for enhancing public trust and safety online with our respective TLDs.

In fact, during tomorrow's Public Safety Working Group session at 6:30 p.m., representatives from the consortium will provide a briefing about our activities.

And, in closing, there are a number of resources provided on the screen and including my email address and phone number. Happy to take questions offline or certainly here in this session as well.

So, again, thanks very much for the opportunity today.

BOBBY FLAIM: Okay. Thank you, Craig.

Does anyone in the audience have any questions specifically for Craig?

Okay. We have one question.

JOHN LEVINE: Hi, this is John Levine. I think you said there were 6,000 registrants. But I just counted. And there are, like, 2900 names in .BANK and 186 in .INSURANCE. So I'm wondering where are the rest of them?

CRAIG SCHWARTZ: Fair question, John. Two of the security requirements for our domains are that they must be DNSSEC signed and they must use in-zone name servers to appear in the .BANK zone. So, for domain name registrants who have not met those two requirements, their domains don't currently show up in the zone. Although, if you did a WHOIS lookup for them, you would find them there.

JOHN LEVINE: Okay. And sort of an unrelated question, is banks and insurance are both heavily regulated, so you can generally go to a regulator and say is this a real bank or is this a real insurance company. I notice that the others you're talking about, like pharmacy and doctors, are also licensed and regulated.

Do you see -- I'm wondering is -- does this model extend beyond industries where you can start with a regulator to find out who is legitimate? Or is that part of the model?

CRAIG SCHWARTZ: Well, I think it probably could. I can only speak to .BANK and .INSURANCE. And one of the elements of the value proposition of our TLDs is that regulated nature and the fact that these entities are all legitimate prior to getting into our space. I'm sure it might work in other spaces, but I just can't speak to them offhand.

BOBBY FLAIM: Michele.

MICHELE NEYLON: Michele Neylon, for the record. Hi, Craig, how are you?

CRAIG SCHWARTZ: Hi Michele.

MICHELE NEYLON: The obvious thing for me with this is going to be down to scale and price. With this kind of policy and process, your domains are only going to be available to a very, very small subset of registrants, be they organizations or individuals.

So, in many respects, as a kind of a model, I don't see how it can scale up to make domain names accessible to a broader public. Or am I missing something?

CRAIG SCHWARTZ: I'm not sure I understand your comment about it not scaling up.

MICHELE NEYLON: Okay. Let me be more precise.

Verifying and validating registrants at the level that you're doing costs a fortune. Therefore, the cost of a domain name registration in any of the TLDs that implement this is going to be significantly higher than a TLD such as .COM. Therefore, logically, people can only register those domain names and maintain those registrations if they are willing to pay a significantly higher price. Therefore, the domain names are only accessible to people with a certain degree of money. That's, basically, what I'm saying.

CRAIG SCHWARTZ: You're exactly correct, and part of the attraction of our TLDs is that exclusivity and the trust and consumer confidence that comes along with knowing who's in the space. And if our TLDs

are smaller, that is by design and we're perfectly comfortable with that.

BOBBY FLAIM: Thank you. Do we have any more questions for Craig? Okay. We can move to the next presenter. One thing I did want to kind of throw out there or ask that goes directly to the last question, and we had asked Craig this before, considering the scalability and how this would work across the entire domain system, and we have heard this before, that it doesn't scale. It's very, very expensive. And to the community -- and Michele and I even had this conversation -- considering that there is a large gTLD auction fund that's out there, is there any possibility that that could be used for any of these efforts? And I throw that out there not necessarily with specifics, but to get good abuse mitigation is going to cost money, and I think if there's available funds, how can we be effective and how we can use these funds directly for domain name registrations and the applications and auctions to actually do that where we're not putting the cost necessarily on a registrar/registry but it goes across the community. So anyway, just a thought. We can again discuss that later. So -- but I guess our next presenter -- not I guess, I know -- is going to be David Conrad, the CTO of ICANN. So David, thank you.

DAVID CONRAD: Thank you, Bobby. Next slide, please. Actually I should say that my team from the office of the CTO incorporates both research activities as well as security, stability, resiliency activities. John Crain, who was one -- back there in the back, is the chief security, stability, resiliency officer and his team is the ones that I'm going to be mostly talking about here.

So we were asked to talk about a number of items, and they include handling of abuse, interactions with contractual compliance, contracted parties, and others, research project on public reporting of abuse, the identifier system attack mitigation methodology document, and improving the state of abuse mitigation. Next slide, please.

So to talk about the SSR team's interactions with contractual compliance and others, the SSR team and contractual compliance right now are investigating ways how we can improve the collaboration. As you may know, we've had a new head of compliance, contractual compliance join -- or well move departments within ICANN. It's Jamie Hedlund, and he and I have actually been discussing ways in which my teams can provide additional support to contractual compliance relating to various aspects of the -- of activities that the contractual compliance department undertakes. In general, the SSR team refers matters that we have knowledge of over to contractual

compliance. My team doesn't obviously have any contractual compliance capability, but when we are aware of something, then we will pass it on to contractual compliance for them to take a deeper look at. And the SSR team regularly reaches out to contracted parties and the operational security community to enable informal collaboration in voluntary threat mitigation efforts. My team, John's team, actually is involved with a number of the operational security trust groups, and those trust groups allow for confidential information to be passed back and forth and it allows for our teams to find out about the various issues that are being experienced and the ways we use our knowledge to actually help mitigate those, when possible. Next slide, please.

We also have an anti-abuse research project within the SSR team. We've hired a third-party contractor to develop a data analysis platform for DNS abuse. It's currently in beta. We, like others, actually obtain multiple data feeds of various forms of abuse that are relevant in the context of the GAC communique. Those include phishing, botnets, malware, and a couple of others that we also incorporate that are outside of the GAC communique because we see them as useful indicators. Not that we have any ability to actually address any of that. We're investigating right now how we can make those results

available. A lot of the data feeds that we receive are considered private information. We've had to sign contractual NDAs and that sort of stuff, so we're trying to figure out ways in which we can make that data available. Next slide, please.

But this is a sort of a screen shot of that beta platform. It's a little hard to read, but it -- you'll see in the slide deck when that gets sent out that, you know, it has a ranking of the gTLDs, including information such as the domains in the zone, the number of listed domains, an abuse score, and this data was from, I believe, March 10, and it shows the relative scorings of a number of gTLDs related to the amount of abuse for which in this context is the listed domains for -- relative to the total number of domains. Next slide, please.

Talking a bit about the identifier system attack mitigation methodology document. That document was created in response to a recommendation from the first security, stability, and resiliency review team. This was an Affirmation of Commitments mandated review that was performed, I don't know, four years ago. I don't recall. Recommendation 12 said, well, an identifier system attack mitigation methodology be created. So the SSR team developed this document, and the steps there are sort of the high level of that methodology. Identify, prioritize, and periodically refresh a list of the top

attacks, develop guidance on high-impact attacks and emerging high-risk vulnerabilities. Describe the attack mitigation practices that correspond with those attacks. And encourage broader adoption of those practices via contracts, agreements, and other incentives. If you'd like to see that document, it is, of course, available from ICANN's Web site, and that's the URL to pull down the PDF. Next slide.

On the topic of improving the state of DNS abuse mitigation, part of the SSR team's role is to produce the sort of unbiased, impartial data and analytics that enable the informed community to provide -- to develop policies that help in related to DNS abuse. And we also focus on sort of the internal side informing the internal organization's various functions on DNS abuse related matters. Both the SSR team and the research group within the offices of the CTO are focused on both of these goals. And next slide.

Improving the state of DNS abuse mitigation, we also provide training and advice to public safety -- to the public safety community, the anti-abuse community, enabling to understand the DNS and how it works. The way ICANN policy development processes are undertaken and the organizational processes and procedures within ICANN as the organization itself. Next slide. I'm on my last slide.

[Laughter]

And I'll pass it over to Maguy.

BOBBY FLAIM: Fabien, can you put up Maguy's slides? I think those are yours. You see them? Okay. Yeah.

MAGUY SERAD: Good afternoon, everyone. My name is Maguy Serad. I'm with contractual compliance. Next slide, Fabien, please.

We received a special request -- a specific request from the Public Safety Working Group to discuss the following topics, and the background of this request is our response to annex 1 GAC communique. Next slide, please.

The first -- the first question was, how ICANN SSR team and compliance department work together. As you just heard from David, the ICANN contractual compliance team works with multiple internal referrals from the ICANN organization. And I've listed a few here, but what I want to emphasize on is what David just talked about. Our team has worked from the very beginning with the SSR team when there are issues of DNS abuse. And the way it works is they refer the -- they inform us of the issue that they are seeing, they refer it to us, and we obtain as much

information from them before we proceed reviewing within the contractual scope and then following up with the contracted party. So all referrals to compliance follow the same approach and methodology. Next slide, please.

The other question was asked is, what specific actions have been taken against registrars. We at the -- in compliance we are very transparent about the different actions we take and publish all of the reports. What we publish is specific to the enforcement actions taken against the contracted parties. During the enforcement phase, which is initiated at a notice of breach, is when we publicly make available to the community what enforcement activities are happening for which contracted party. What I wanted to say is, in addition to a specific issue that is in breach, what we do in contractual compliance is before we issue a notice of breach, we do a compliance check, which is a full check of the state of that contracted party. We review what are the other areas of possible noncompliance issues, and we built all of that into the notice of breach so we address the entire issues together versus just one issue at a time.

In 2016 -- and this data can be found in our annual report -- we had 25 registrars who received a notice of breach. The details of each of the breaches are listed. The most important question here is, what actions are taken to promote increased

compliance by registrars? I have provided a lot of slides in this presentation, but to summarize it here is the most -- the best way to promote increased compliance is the increased proactive activities that the contractual compliance team initiates. We look at the state of the compliance world, where are we seeing trends, where are we seeing consistency in issues and opportunities to do outreach, whether it's outreach by topic or by region or by even the level of just very focused outreach with a specific contracted party.

So it goes from a bigger picture to a targeted outreach effort. And what we also do to promote increased compliance is that if and when a compliance matter has been addressed in the past and we find out that the problem is surfacing again, we go immediately to an escalated notice with the contracted party. Because that issue should have been resolved and addressed. And the other way of also increasing and promoting compliance, being in compliance, is the proactive audits that we conduct. It's a proactive way of identifying issues, getting them addressed or clarified, and mitigated hopefully and avoid a repeat of those issues. Next slide, please.

I've provided a few slides of data here. Just -- I'm not going to go through them. Next one, please, Fabien. One more.

This is the details to support a response we provided to the annex 1 GAC communique about the 30,000 complaints -- 32,000 complaints between November 2015 and 2016. Based on our conversation you wanted to understand the breakdown of them, how many were received and how many were closed. But what I would like to highlight in this table is that we received the volume that you see on the left most under column received but you would need -- what you also need to look at is, we do vet and review the complaints before sending them on to contracted parties. And therefore you see there is a column referred to as closed before first notice or before a first inquiry.

And the volume there, you see it. And why do we do that? Is because sometimes we receive complaints that are not complete or they're not within the scope of the allegations, or the complaint that's being filed with us could be on a domain name that's either suspended or no longer valid or deleted.

So we have all the closure reasons available in the presentations that we publish on our website.

What I've also provided to the audience, which is something really that you don't probably review it in that view, we all hear about the informal resolution process. Compliance publishes aggregate members about the informal process. But what I wanted to bring to this audience is an appreciation that goes on

between first, second, and third notice before a notice of breach has happened.

Look at the volume of complaints in first notice. After we go through the first step, you notice, you start -- I'm just going to take the WHOIS inaccuracy. 14,000 -- almost 14,000 complaints in first notice. And what this story is saying here is the fact that that number is much, much less in second notice, it means that the issues that were brought forward in the first notice or the first inquiry have been resolved.

What goes into the second notice is the 1340 -- 1,340. What happens here is if a contracted party does not respond to a compliance notice at all, it will move to the next phase. If complains received an incomplete response from a contracted party at the very last minute, then it goes into the second phase.

So what the message here is, from 14,000, now we're down to 1300. And the same principle applies. We have about 160 that go into third notice.

Our goal here is to make sure that the issues brought to the contractual compliance have been reviewed, addressed, and hopefully resolved, if not closed ultimately at the end.

So I just spoke a little bit more to that, Bobby, because you guys had asked for that.

Next slide, Fabien, please. Yes, I'm finishing. Fabien. One more, please.

That's for you guys to take a look at.

One more, please, Fabien.

This is the monitoring activities that we conduct, and it's just to show you what are the sources that we depend on when we conduct monitoring activities.

One more, please.

I highlighted a few outreach activities we conducted in 2016 as information for you. All this also is available on our website.

With this, I conclude my presentation. Thank you.

BOBBY FLAIM: Okay. Thank you. Sorry. I apologize for rushing you, but we only have about 12 minutes and we wanted to see if anyone from the audience has questions, actually, of everyone who is on the stage or -- Yes, sir.

JOHN CARR: John Carr from the European NGO Alliance for Child Safety Online. I was very much attracted by the first presentation

showing the high level of security and verification that was being put into confirming the identity of certain registrants and so on, and I'll give a concrete illustration of why.

We've been following the .KIDS gTLD process for some time. It's still not been resolved, as you'll know, but we did discover about five months ago that in fact .KIDS has already been let in the Cyrillic script. So there is a registry based in Russia called .DYETI, and I wrote to them and I asked them the two -- these two questions. When selling a .DYETI registration, do you make any stipulations about who may buy such a domain? For example, nobody with any convictions for child sex offenses. And if you do, do you take any steps to verify that that is correct?

Second question I asked was do you make any stipulations about who may work for a business or organization that operates a .KIDS or .DYETI domain? And if you do, do you take any steps to verify whether or not that is the case?

The answer to both questions was no. They make no stipulations of that kind, and so obviously it follows neither do they try to verify whether that condition is being met or not.

That seems to me that ICANN has failed in its duty of care to children to ensure that in the registry agreement that was issued to .(saying name) that conditions much that kind were inserted.

And I think it's symptomatic of a wider failure by ICANN, but I can see how, if we could get .KIDS accepted as being a high-level security-type issue and it could be part of a regime like the verified TLDs is for finance concerns, that would allay most of our fears or concerns. So it's a general question linked to a general comment about how, to what extent it might be possible to achieve something of that kind.

DAVID CONRAD: I'm not sure exactly how to answer that question but I will say that one of the processes that is being undertaken currently is coming up with procedures associated with the next round. And that might be an area that could be focused in terms of requiring additional registrant information.

With regards to the existing gTLDs, I'm not, obviously, a person to talk to that as I don't have background in the -- in the contracts or the -- the legalisms that went into the definition of who could register or not within one of those top-level domains. So I'll have to defer that to probably, I guess, our legal folks.

CATHRIN BAUER-BULST: Thank you.

Now, before we go to the floor mic, I have one more remote participant person. From Steve Metalitz to you, Greg. He says: Thank you, Greg, for your presentation. You stress the importance of contracts and enforcement by industry players of terms of service. Some have attacked such enforcement as shadow regulation by private parties and have called for an end to such voluntary arrangements. Do you have any response to such criticisms?

GREG AARON: I think Steve is referring specifically to enforcement of trademark, and that's a very specific area that is distinct from cybercrime.

I think the issue was settled a while ago that dealing with phishing and malware and other criminal issues, that there is a role for the community. And as I said, you know, a lot of parties, like registrars and registries, have been dealing with those issues for a long time.

Steve's referring to trademark, which is a different issue, more of a civil issue.

CATHRIN BAUER-BULST: Thank you, Greg.

Please, go ahead.

KEITH DRAZEK: Thank you. Hi, everybody. My name is Keith Drazek. I work for VeriSign.

I just had a question about whether you all have also focused on the issue of domain hopping. This was something that was identified by the White House Intellectual Property Coordinator's Office, and it's basically a practice of criminals or those infringing on intellectual property using the Domain Name System, jumping from one TLD to the next to the next to perpetuate their ability to be able to continue the abuse.

It's not specific only to intellectual property, but, you know, Greg, you mentioned in your report that there were these instances of tens of thousands of domain names being registered. In those instances, whether it's, you know, one, ten, or 10,000, where the criminals are actually taking their elicit behavior from one TLD to the next. And I guess my question is is there an opportunity here for ICANN to help industry players, registries and registrars, collaborate and communicate to identify instances where these bad actors are actually identified, identified in a particular TLD, and that's gTLDs and ccTLDs, and then to be able to try to identify this bad behavior, communicate

to identify where they may be going and somehow address the challenge of having to essentially chase the criminals around the world as they move from TLD to TLD.

Thanks.

GREG AARON: Thanks for the question, Keith. Right now there are something like 365 million domains in the world in all the registries, and Keith Drazek.

KEITH DRAZEK: And as you say, criminals will buy domain names as disposable resources. They'll use them sometimes immediately after registration. Sometimes they'll wait months. They hope for their domains to be registered for a while and therefore gain some certain level of reputation, and then they'll start using them.

It would be a coordination effort to try to identify those people. And those people are also using false identities. They're faking their WHOIS information, for example.

One of the things we need to do is make sure we have access to information. The continued availability of WHOIS information is a big topic right now at ICANN, and we need to see how privacy

regulations may be able to co-exist with making the information available where possible. So that's a big issue ICANN has to deal with right now. And I can't stress the importance of that information because without that information, it's very difficult to identify what's going on and make attributions.

It's also difficult for people to track these people in what they're doing day to day and say this person was here in one place and now they're at another. It's a practically difficult job and it would require some really concentrated funds and resources in order to accomplish, I'm afraid.

CATHRIN BAUER-BULST: Just one point to add on that before we go to the next question. I think it's a really interesting idea and something we also see in other context, such as content takedown where there are also efforts being made to avoid illegal content doesn't pop up elsewhere.

And in the context of child sexual abuse, the solution was developed that many of you are probably familiar with called Photo DNA. We don't actually store the actual materials, but rather you create hash values on the basis of the materials that are robust enough to also be able to be compared to images that have been slightly modified. And they also circumvent the

personal data problem because you're not dealing with personally identifiable information but, rather, with a hash value that can be recreated. And maybe there's a way of also storing information on bad actors in a similar manner. And again, maybe we can have recourse to some of the immense funds that are available from the auctions to help work on some of those big challenges.

And with that, I turn it back to the floor. We're going to be able to take the next three questions and then I'm afraid we're going to have to already close the session.

Please.

JOYCE LIN: This is Joyce Lin from 007names.com.

I think it's great and dandy that you have the data analysis for all the DNS abuses, but I think the tougher part is the enforcement. And currently, the enforcement, it seems to me, is all on registrars' burden, on registrars' shoulder.

I can give you an example that we recently received email from LegitScript which they are monitoring all the illegal drug sales on the Internet, the prescription drug or the fake drugs. So they sent us an email, say, hey, you have 12 names that are doing

illegal pharmaceutical product sales. And we try to be a good player, try to help, so we immediately identify the registrants and send them the email, say, hey, we got this complaint about your domain name. You are violating the -- our service -- registration service agreement. And according to the RAA, the contractual obligation, we are supposed to give them 15 days to correct the issue; right? But, boom, within two hours, three domain names moved out.

And so what are we going to do? As the registrar, we lost the sale for future renewal, and in the meantime we are not resolving any issue at all.

So it just -- to me, I feel like an idiot because I showed my customer out of the door, but I wasn't helping LegitScript to resolve the issue that they go after us for that.

And you know what? I think that ICANN should probably think about another way of placing the burden in terms of this kind of abuse. For example, we have about four or five names that -- when I say that, should go to the registry instead of the registrar for this kind of enforcement. We have about four or five domain names. All of a sudden we didn't know what happened. Customer cannot modify, they cannot renew it. So we look into the registry and we found out it was the court order that was suspended.

So very sensitive. Sorry; it's a court order, you still have to pay for us. But our customer didn't want to pay for it so we got stuck. So how do we know how long this court order is going to be there for this domain name? It might be for the rest of my lifetime, so that means that we have to pay for that; right? Which is another issue.

But the point is if ICANN or whoever the legal authority has identified all the names, they should go to the registries, say, okay, those are the names in your sponsorship. You should suspend them, you know, put them out of the zone file. That will be a more effective way to do that. Otherwise, you don't have to jump from TLD to TLD. You can jump from registrar to registrar and there are 2800 registrar all over the world and it's open loop there. They can loop around. What are you going to do with that?

Okay. Thanks.

Contract compliance could come up with maybe a list of -- I don't know -- bad actors to keep them out of the DNS? Is that something that is possible?

DAVID CONRAD: One of the joys of the Internet is, when you're on the Internet, no one knows you're a dog. Similarly, no one knows that you're a

criminal without, you know, some other external identifying information.

A lot of these issues are very difficult to identify solutions. And ICANN the organization relies on ICANN the community to help us identify mechanisms by which we can address the issues that are affecting us all.

With regards to domain hopping, there may be ways in which sort of big data associated techniques may be able to suggest some potentials in which a particular set of domain names are likely to be hopped from one TLD to another. And that might be able to be fed back to registries or registrars as, you know, potential ways of identifying potentially vulnerable top-level domains.

But then the question becomes: What do you do with that information? Do you block those domains from being acquired by someone who might have, you know, a perfectly valid reason to do so? Or -- the questions there start getting very complicated.

You know, with regards to the registries versus the registrars, who should receive notices, there's clearly some areas in which communications could be improved and sort of the abuse notification chains and those sorts of things.

That's something that one of my team are actually sort of looking at sort of the lifecycle of domain name abuse and how to address that.

And that -- the information that we collect within the organization is then provided back to the community as information to help them in the policy discussions, which, basically, means that don't expect an answer any time very soon. But it is something that we hope to be able to help the community in their deliberations.

CATHRIN BAUER-BULST: Please go ahead.

KAVOUSS ARASTEH: My name is Arasteh from GAC. I would like to give a different angle to this situation. Perhaps we're dealing with the issue in a piecemeal approach, not in a long-term strategy approach.

The measures which have been taken, including mitigation, seems -- does not cope with the speed of those anti-abuse issues. Maybe those are going more faster than you or they are more clever than us. Maybe they are more brighter than us in the bad doing things.

So we need to change our strategy. We need to look at the matter in a more coordinated matter.

Until the time that we do not see a tangible reduction in this anti-abuse measures, I don't think that we could have any confidence that what we are doing is proportionally replying to the matter. Maybe we cannot stop that totally. But it means that a statistic that you show, I can tell you in the room, is going exponentially.

So what does it mean? It means our measures need to be reviewed. Please, kindly, don't take it as any criticism. Take it as some sort of warning that perhaps we need to look at the matter from different angles to see what we can do.

Someone said that the complaint has not been processed because they were not complete. It is an issue. You just have validation tools for the complaint. Any complaint before being sent to the ICANN must be validated. If it is not validated, something incomplete, it is not a complaint yet.

So you should avoid to have received something and being recorded as non-treated yet. So there are many other measures.

Apart from that, there is a need to really look whether there is a willingness of all parties to do something.

I have some doubt of that willingness. I have seen many measures, many discussions from 2007 starting from somewhere outside the ICANN under the cybersecurity agenda, which was the result of two years of study. But some people reject that saying, no, we cannot apply that because internal issue, is internal policy, so on and so forth.

So perhaps we should look at that, one to see; one, whether there is any willingness of all parties; two, whether we could have a long-term strategy; three, whether the measures we have to take is corresponding to the appearance and the occurrence of those things. And, if there is no significant reduction in the number, that means our process has failed. It is not your problem. It is our problem. It is a collective fault, and we have to look at that again. Thank you.

CATHRIN BAUER-BULST: Thank you, Kavouss. Did you want to react? Yes.

MAGUY SERAD: Hi, Kavouss. This is Maguy Serad. I would like to address the one item you said about the incomplete complaint. Basically, what I was trying to say earlier is that, when we receive complaints from outside, we vet them to make sure that we have the right information.

So sometimes people don't provide enough information or don't provide us evidence. We go back to the reporters and we say can you please provide more information. It's not something that can be automated because the cases are so diverse. I just wanted you to know that it's not just incomplete and we close it. We do follow up with the reporters to make sure we are trying to obtain as much information so that, when we send the issue to the contracted party, they have information to base it off and address it.

Thank you.

CATHRIN BAUER-BULST: Thank you, Maguy. Please go ahead.

ALAN WOODS: Thank you. Alan Woods, Rightside Registry. It's just in relation to the beta program that you mentioned with the listing of the abuse that was showing up on various TLDs.

I suppose I have three queries, could be questions, could be things that need to be thought about.

The first one, I suppose, is: Who are the third parties that you are basing the data on? From a registry point of view, many registries out there. Many of us have the spec 11.3b

requirements. And, within the requirements, every single one of us potentially has a different view upon the blacklist providers, depending on the blacklist providers that we ourselves consume.

One of the questions we've always asked is: Well, are there ones out there that maybe are better to look at? And we've never received an answer. And to see going up on the screen a -- an aspect, not from a registry but from ICANN, of a selection of the blacklist providers, it gives me pause for thought as well. Because, yes, I believe that we should have a knowledge and an idea of what is underlying and how many abuse cases are potentially out there. But, at the same time, we must be absolutely clear that a listing on a blacklist provider does not equal something that is actionable by a registry because we have no view of the evidence that is -- that that report or that abuse report has been based upon.

We cannot -- we can't just say, you know, this is on a blacklist, therefore, I can action it. That is not a thought process we must investigate.

So the three points, I would say, is what is the purpose of this beta program? The second one then is are you -- is there a tantamount acceptance that certain blacklists out there are of

better higher quality and ICANN have tested and trusted these people?

And then I would ask how is that going to interact with the registries and how we are currently applying our obligations in a way which we see fit?

CATHRIN BAUER-BULST: In view of time, sorry -- thank you very much. I would propose, if the last question -- if you can make your question in 30 minutes and then I'll give you time to respond to both, if need be.

UNKNOWN SPEAKER: 30 seconds.

CATHRIN BAUER-BULST: Okay. Go ahead.

UNKNOWN SPEAKER: That was a good question, though.

CATHRIN BAUER-BULST: Oh, 30 minutes. Yeah. We can also take 30 minutes, but 30 seconds would probably be even better. Sorry about that. Please, go ahead.

VOLKER GREIMANN: Volker Greimann. Key-Systems, registrar. As a contracted, it's sometimes hard to look at a complaint and see the whole picture. Because we're not experts on abuse. We're the experts on selling domain names, managing domain names. We get an abuse. We don't know if it's illegal, what's happening there or if it's just illegal in a certain country. We don't see the whole picture. Sometimes we're asked to take down a Web site, and we do it. And then we get a call from other law enforcement agencies that ask us what the hell we're doing. They're investigating the Web site, and please turn it back on.

We do not know what is going on with that Web site. We have an indication what can happen. But, ultimately, when we have to take a decision regarding an abuse complaint, we're always ending up holding the short end of the stick because no one is indemnifying us for a mistaken action that we might be taking or non-action that we might be taking.

So it's a very hard decision that we have to take on our own economic risk and our own social risk and our own legal risk.

DAVID CONRAD: So, in response to Alan, the genesis of this research project was actually a report that was published, I believe, from a company

called Blue Coat that actually documented or provided statistics on DNS abuse that were highly questionable.

And the methodology that they had used was deemed not to be particularly effective in coming up with sort of a reasonable estimation of the amount of abuse a registry was being subjected to.

So the intent of our project is to collect data from as many feeds as we can possibly get. We don't have a limitation on the number of feeds that we will be importing into the system.

And to document a methodology publicly that the community can see and agree upon about how the metrics are established. The intent of that is purely informational. We will have a set of data that will show behaviors over time. And ICANN will not -- my team, as I said before, has no contractual compliance responsibilities. That's not our job. But it is intended to provide information to the community that the community can have some trust in as to what level of abuse is affecting particular registries.

And, as -- with the intent and the hope that the registries will be able to use that information to work within the community and within the policy processes to improve DNS abuse, well, to

improve the mitigation of DNS abuse moving forward. And I guess I'll let Maguy answer the second question.

CATHRIN BAUER-BULST: I think we're, going to have to close the session because we're already over time. Sorry, Maxim.

This just goes to show that this is a really key conversation we should probably continue having in some form or another.

Some key takeaways I have, before I turn it over to Bobby, from today is that there is not enough information.

There is sometimes conflicting information. There's not necessarily agreement on what should be authoritative information.

One thing I was going to suggest for the cooperation between the SSR team and compliance was that something like the abuse score that we just saw where, you know, some of the registries, some of the TLDs were actually quite high with, I think, 48% and more for .SCIENCE and others, that would, to me, as a lawyer, sort of trigger compliance action automatically.

However, if we cannot agree on the validity of the underlying information, it creates some challenges also for compliance and acting upon it. Perhaps we, as a community, need to have a

conversation about what we consider as reliable information but then also what steps ICANN compliance should be taking on the basis of that information. And the GAC and others probably have a key role to play in that.

And then we have to look at how we can improve cooperation. Because what also very much resonates is that different parts of the community feel overburdened with the role that they're expected to play in this process. So we have to see what we can do as a community to mitigate that responsibility. Mitigation being the key term today, of course. So now I turn it over to Bobby for the final words.

BOBBY FLAIM: Thank you, Cathrin. First of all, I want to thank all of our panelists -- Maguy;

Dave; Craig, who is participating remotely and also Greg. So thank you all. I thought they all did great presentations, and they were very illuminating.

Just to add on what Cathrin said, we do have a few things that go directly to DNS abuse mitigation. The GAC PSWG does have some further questions concerning Annex 1. So we're hoping to get more information based on that.

Also to highlight the CCRT and their DNS abuse mitigation or DNS report. So we want to highlight that. And that will also be very, very helpful. And also to see -- to go to what Kavouss was talking about, what Keith and what Joyce were talking about to see if there could be some systemic or enterprise level approach to the abuse to assure that registrants, in particular, that have nefarious purposes are not allowed to use the DNS system and how we can work with registrars and registries to do that. And, again, hopefully, we can use some of the money that ICANN has through those auction proceeds, once again, to see if we can foster that so it won't be a burden on anyone in the community.

So thank you all very, very much. We appreciate your time and attendance and especially your participation. So thank you very much.

[END OF TRANSCRIPTION]