HYDERABAD – High Interest Topics session: Mitigation of Abuse in gTLDs
Saturday, November 05, 2016 – 13:45 to 15:00 IST
ICANN57 | Hyderabad, India

ALICE MUNYUA: Good afternoon, everyone. This is the high-interest topic session that has been organized and hosted by the Public Safety Working Group of the Governmental Advisory Committee.

My name is Alice Munyua, chair of the Public Safety Working Group with the GAC, with the African Union Commission.

I'm going to start off with a quick introduction of distinguished panelists here.

Start from the -- right there, please. Your name and the constituency. Michele.

MICHELE NEYLON: Michele Neylon, registrar.

BRIAN CIMBOLIC: Brian Cimbolic, registries.

STATTON HAMMOCK: Statton Hammock, registries.

CARLOS ALVAREZ: Carlos Alvarez, SSR team, ICANN staff.

GIOVANNI SEPPIA: Giovanni Seppia, EURid.

DENISE MICHEL: Denise Michel, business constituency.

ALLEN GROGAN: Allen Grogan, ICANN contractual compliance.

DREW BAGLEY: Drew Bagley, Secure Domain Foundation.

BOBBY FLAIM: Bobby Flaim, FBI, Public Safety Working Group.

FABIEN BETREMIEUX: Fabien Betremieux, ICANN staff, GAC support.

RICHARD ROBERTO: Richard Roberto registries.

ALICE MUNYUA: Thank you very much, and you're all welcome.

Just very briefly, the GAC Public Safety Working Group was created in 2015 during the Singapore meeting, and the main time of reference is it focuses on the aspects of ICANN policies and procedures that implicate the safety of the public.

So we'll just go straight to the session, because we don't have that much time and we'd like to have interactive discussions.

This session we're focusing on mitigation of abuse in gTLDs. And the goal and expected outcome of this session is we're going to be providing an update of the -- by the ICANN community and its supporting organizations and advisory committees on current industry best practices in the mitigation of abuse in the DNS.

We are also going to have an update of ICANN community and its SOs and ACs on the current status of relevant activities, including sharing of available information, the effectiveness of it, of current safeguards, and abuse-related undertakings that are still in development. And then provide an opportunity for us as an ICANN community to raise concerns and present any views for consideration going forward, and especially for input in current reviews and activities.

So the agenda, as you see there -- oh, sorry.

We're going to start off with a definition from the Public Safety Working Group, Bobby Flaim.

So, Bobby, please. You have the floor.

BOBBY FLAIM: Thank you, Alice.

I think when we talk about abuse, it's almost like we had a judge in the United States trying to describe or define pornography as kind of you know it when you see it, and I think that's what you could also use for abuse or misuse concerning the DNS.

Some of the things that we have listed there actually come from the Public Safety Working Group, actually the GAC safeguards. And you see pharming, phishing, malware, botnets. But that really is not an all-inclusive list. That goes to some of the technical aspects of abuse.

Abuse and criminality actually varies from country to country. We have to consider the national laws because we still do live in a world with national laws and what may be a crime in one country would not be a crime in another. The fact that there is child exploitation on DNS, there are websites that we see that are being used for terrorism. We've all seen them on TV.

So there's lots of different types of abuse, and there really is no one solid definition. And I think that's the most important thing that we have to consider when we're looking at the DNS and the public safety of the DNS.

So we hope we have -- Well, I don't hope. I know we have a very good panel. And one of the purposes that the public safety had was to get the perspective of the operators of the DNS, the registries, the registrars, ICANN itself. There's security, their contractual compliance, so we can actually see what is being done out there, what are some of the best practices to ensure that we're preventing and mitigating abuse on the DNS, especially as it relates to the ICANN ecosphere.

So we are very confident that this will be very informative and productive, and we look forward to the conversation and some of the discussion that we're going to have today, not only the speakers but also you in the audience. So we are really looking forward to your participation.

So without further ado, I'm going to introduce to my colleague Drew who will actually go into maybe some of the illustration of some of the case examples, full, of abuse.

So Drew.

DREW BAGLEY: Thank you, Bobby.

So I'm speaking from the perspective of some of the abuse trends that we see at the Secure Domain Foundation, which is a nonprofit organization that specializes in proactive anti-abuse.

And, you know, DNS abuse is something that is important not just in the world we live in in ICANN but it's something that affects so many people around the world in terms of the victims of the latest trends of cybercrime.

And so many of the things -- many of the headlines that we hear about today actually start with something at simple as a domain name registration. As Bobby mentioned, the technical definitions of abuse are generally more narrow, and when you think of phishing, pharming, malware hosting, botnet command and control, and spam. And so those are the ones that I'm going to focus on as far as trends are concerned, even though DNS abuse, of course, can affect so many other things.

And something that has been a trend as I'm sure everyone is aware of over the past several years is that DNS abuse is now having large-scale financial ramifications like never before, instead of it just being that -- you know, isolated to maybe single victims and a much smaller scale micro trend. So we're now at the point where DNS abuse is actually affecting, to some degree, the stability of the DNS system.

Some of the newer trends, especially from this past year, and some of the headlines that I'm sure many of you have seen in recent months, have been of course ransomware, which takes many different forms but two of the most popular variants of

ransomware are Cryptolocker and Locky; business email compromise; and the Internet of things, botnets, which of course have especially been in the headlines the past two weeks.

So ransomware is something that started off I think much smaller where individuals were being targeted when they would visit a website or click on a link and their computer would be encrypted and could only be decrypted if they paid a ransom.

But now this ransomware trend has affected even large businesses, it's affected hospitals. And so what it's led to around the world is something that actually has become an issue where a business can lose effectively all of its intellectual property instantaneously and its ability to run its business when their computers are encrypted unless they pay the ransom. So because of that, victims generally tend to pay ransoms in these instances and it's become a lucrative business for cyber criminals. And some of the latest statistics show that the infections are going up rapidly. In March 2016 alone, there were 56,000 infections just in that month, and so that was twice as many as what was going on the preceding year where you had at least 23,000 infections per month. And the amount of money that's been paid so far is over $200 million.

And another trend within this ransomware variant is ransomware is now being offered as a service. So you don't

have to actually know how to Unicode yourself. You can just pay to use the ransomware to target victims and make money.

Another trend I mentioned, business email compromise. So this is a form of carefully crafted social engineering that goes after business executives, targets them with phishing emails that look like they're very legitimate because of the fact that they're written in the same style as the employee they purport to come from and whatnot, and, ultimately, oftentimes result in a financial transaction taking place where the business executive thinks it's a legitimate request from the accounting department, okays the transaction, and then that money is stolen by the criminals. And according to the FBI, there have now about over a billion dollars in losses due to this.

And the Internet of things, botnets, which we have seen in recent weeks with the Dyn attacks and the Liberia cyber attacks. And unfortunately my time is running out so I will kind of close with these trends really happen in two ways, where perpetrators will take over legitimate websites but what's much easier is for a cyber criminal to register their own domain name. And so one of the more recent trends is for them not to use a registrar to register a domain name but, in fact, to go to a reseller that accepts Bitcoin and offers privacy and proxy services. And at that point you're a bit removed, too, from ICANN, so even though resellers are, of course, included within, you know, the

responsibilities of registrars and registries, resellers themselves don't have a direct contractual relationship with ICANN. And so you're really seeing a very interesting trend happening on the periphery that's absolutely affecting some of the biggest cyber criminal -- cybercrime trends we're seeing.

And I now yield my time to the next speaker.

Thank you.

BOBBY FLAIM: Actually, before we go to the next speaker, I just wanted to ask you a question. Based on the trends that you're seeing, especially this DNS threat sector and the use of Bitcoin, do you think -- what do you see as a possible solution to some of these threat vectors?

DREW BAGLEY: So I think one of the main solutions would be proactive anti-abuse mitigation. I won't have time to go over these slides but I could at least put it up.

But essentially, even when you don't have good data to work with, you might have bogus credentials in WHOIS where you may have the privacy and proxy, you're still going to have some common data because bad guys have to scale like anyone else

so they will use the same email addresses over and over again. So I think there's obviously putting pressure on privacy and proxy providers, in the face of good evidence, of course, to unmask or in some other form share data on the registrants and then also to utilize the common bad WHOIS data so that you can stop repeat registrants. So that you can't just keep using the bad credentials over and over again and get away with it.

BOBBY FLAIM: Okay. Thank you. Our next speaker is going to be Allen Grogan and also Carlos Alvarez. I think you guys are going to do it consecutively. So Allen.

ALLEN GROGAN: Sure. So high level, ICANN's contractual compliance department enforces the contracts that we have with registrars and registries, and those include provisions that are designed to combat various forms of abuse.

Because this is the first ICANN meeting post transition, I wanted to take a few minutes to kind of set a frame of reference, because I think there's going to be an ongoing debate in the community over ICANN's role in combating abuse, and I'm not going to try to answer that question. I'm just going to try to frame the question.

So, under the new mission and bylaws, there's now an explicit prohibition on ICANN acting outside its mission. And I'll leave it to you to review the mission. But, oversimplified, that mission is largely technical in nature and relates to the coordination and allocation of names in the DNS, facilitating the DNS root server system, coordinating the allocation and assignment of Internet protocol numbers and autonomous system numbers and so forth. There's also a new explicit prohibition on ICANN's regulation of services. They use the Internet's unique identifiers or the content that those services carrier provide and an acknowledgment that we're not a regulator.

But there is -- in terms of my opening remarks that we're enforcing the existing contracts, there is what amounts to a grandfather clause regarding agreements that were entered into prior to the transition date. So prior to October 1st of 2016. Or agreements in substantially the same form that were entered into after that and any renewals of those agreements.

I've set forth in the following slides a number of the provisions that are contained in our contracts with contracted parties governing abuse. Just in thinking about this and what ICANN's role is in combating abuse, remember that, whatever our actions are, either need to be within the scope of the mission and bylaws or they need to be contained in these contract provisions.

And I'm going to turn it over to Carlos and let him take the rest of the time.

CARLOS ALVAREZ: Thank you. That's mine.

I'm a member of ICANN's security, stability, and resiliency team. We do anti-abuse work, collaborating with the operational security community and law enforcement community as well. Our focus is not contractual. That's for Allen's team.

We focus our efforts in voluntary cooperation. And our focus is specifically on malicious activity that relates to botnet, command and control, monitor distribution, and phishing. Anything that's not within these categories, it's outside of what we do. We don't do trademark stuff. We don't do corporate stuff. We don't do anything related to freedom of expression. That's not us just in case to make it clear up front.

I'd like to focus here very quickly on some of the things that we do. It's just some of the things that we do that I think it's worth mentioning here.

One of the recurrent things that we always are working on is to provide training to law enforcement agencies, to cyber units with law enforcement agencies all throughout the world. Every week someone from our team is in some country in any of their

regions training police officers from the basic DNS fundamentals to more in-depth investigations on matters that may relate to threats to the system, to the DNS system as such.

Recent examples: DOJ, the Department of Justice in the U.S. in Georgia a couple times; Underground Economy; Austrian Cybersecurity Competency Center; Middle East. We partner with the OAS, Organization of American States. We also have an on going relationship with the Organization for the Security and Cooperation in Europe, OSCE. In Latin America this year we've been in several countries, including Peru twice, Costa Rica, Colombia. We do more. These are just quick examples.

We support the work of the operation security community in the law enforcement in different ways. We provide them advice when they reach out to us with regards to investigations that they're working on that involve DNS resources. We're not interested in what they're investigating. They just ask questions with regards how the DNS works. And we answer those questions for them. They sometimes get stuck and they just don't know how to go about the DNS, so we explain to them. We help them understand ICANN's contractual framework.

The anti-abuse regulations that are in the RAA to clear their expectations, know what paths they can utilize to submit reports of abuse to the registrars, for example. We also assist

law enforcement and our OpSec, as we call them, our OpSec colleagues when they are submitting ERSR requests. These are the requests under ICANN's process and an ICANN process that's called Expedited Registry Security Requests. That's an example of a very successful ICANN process that helps address abuse. Two recent examples are very large take-downs of Cryptolocker and Gameover ZeuS. Those were two very bad botnets that were taken care of by law enforcement and the security community a while ago. And we provide advice to the staff and the community. And recent, actually, ongoing examples are the well-known Spec 11 3(b) work and the registry security framework. We're asked to provide subject matter expert advice. We provide it.

Literally, if any of you has questions with regards to SSR issues, you may come to us. That's why we're here for.

Some of the challenges that we're seeing -- and I have one minute left, which is not very much. We see a registrars and registries with different systems, different implementations of processes, different resource availability, and different levels of expertise. We also see that complainants, the people in the security community and law enforcement sometimes submit reports of abuse that may not be clear, may not provide enough information or simply false positives. That happens. And also there's no standardized reporting of abuse. That's something

that makes life harder for both registrars and law enforcement and OpSec folks.

And also we see a lack of understanding of anti-abuse provisions in both sides, in the complainants and sometimes registrars. It does happen occasionally. So it's worth mentioning.

Something else worth mentioning, there's no uniform terms of service or abuse policies across registrars. So might have more stringent or more strict terms of service with their registrants. Some may have more lenient in terms of service with their registrants. So there's no uniformity there. And big complications in obtaining data for research.

Very quickly, aspirations, we aspire to have a more clear definition of what constitutes DNS abuse.

Probably the PSWG, as well as other parts in the community, could help define it better in a way that's according with the ICANN model.

And research and standardization of abuse reporting processes, that should be positive, aiming at making life easier for both registrars and the complainants. And that's all for me. Thank you so much.

BOBBY FLAIM: Okay. Thank you, Carlos. I just wanted to get Drew in one more time, because Drew is actually going to leave us. Drew, you had a point to share also about DNS abuse mitigations. So, Drew.

DREW BAGLEY: Thanks, Bobby. I wanted to briefly emphasize that beyond the role that ICANN can play and then the roles that law enforcement and other parties can play, it's really important for registrars and registries to share data with each other, whether that is directly or through trusted third party organizations, through trusted non-profits. But it's very important for suspended domain names and that common data that I was referring to that goes along with the purpose. It's important for that to be shared across the community. Because only by sharing that data is it possible to really slow down the bad guys and, you know, utilize their patterns against them.

And so, whatever the takeaway is in terms of the different roles different parties can play, I think it's really important for the community to look at themselves and see what they can do with the data they have to be a force for good and for, you know, helping each other out and making the Internet a bit more safer through cooperation.

BOBBY FLAIM: Okay. Thank you, Drew. Just a couple more questions for Allen and Carlos. Do you see, now that we're entering the post-IANA world, that there might be more pressure insofar as self-correction, contractual enforcement, more proactive security measures?

ALLEN GROGAN: Can you kind of expound upon the question? I'm not sure what you're asking. Sorry.

BOBBY FLAIM: Now that we're in the post-IANA world and ICANN independent -- we'll use that word -- do you see that the community may look upon you more to do more? Now that you're independent, there's more self-correction, more self-regulation, more contractual enforcement, since there's no -- there's no quote, unquote, oversight?

ALLEN GROGAN: What I suspect is going to happen in the new post-IANA world is there's going to be substantial debate in the community about what ICANN's role is in combating abuse. I'm not sure where that discussion in the community will lead. I think there are different constituencies within the ICANN community that have very differing points of view on what is within the scope of

ICANN's mission and remit and what's outside. And I think the post-IANA with the changes in mission and bylaws and the slides that I went through at the beginning of this, I expect a robust debate on that with some people pressuring us to do more and some people pressuring us to do less.

BOBBY FLAIM: And Carlos.

CARLOS ALVAREZ: We hear from our colleagues in the operations security community and law enforcement that they have, indeed, a wish for ICANN to be more active with regard to anti-abuse. So I guess the question is for the ICANN community to address the issue and determine what ICANN's role with regards to abuse should be. That's my take, I think.

BOBBY FLAIM: Okay. Thank you.

Okay. Next we have Statton and Brian who are going to represent us or discuss some of the registry best practices or DNS mitigation strategies. So I think, Statton, you may be first.

BRIAN CIMBOLIC: Actually, I am Bobby.

BOBBY FLAIM: I apologize.

BRIAN CIMBOLIC: Hi there. I'm Brian Cimbolic, deputy general counsel Public Interest Registry. I help manage our anti-abuse program. Our abuse program really begins and ends with our anti-abuse policy, which covers technical abuse of the DNS along with child exploitation. And along with our back-end provider, Afilias, we have both proactive and reactive measures to try to mitigate abuse.

So for reactive measures the first line of defense is our abuse alias. Abuse@pir.org. It's monitored all waking hours 365 days a year, east coast time. We have eight individuals monitoring this to make sure nothing slips through the cracks. And either myself or our general counsel, Liz Finberg, will directly handle the abuse inquiries. Usually, if we get a referral in business hours, we typically have a 1 to 2 hour turnaround to begin our investigation or respond and say this doesn't actually fall under our policy. And, if it's not working hours, 8-12 hours at the latest.

For how we get our inquiries, typically, they come in through end users, law enforcement, and or organization referrers. The

majority of end-user referrals usually don't actually constitute abuse. They'll write to the registry either thinking we're the registrar or they want us to intervene on a domain name registration and it expired and someone else registered it. We let them know that that doesn't fall under our abuse policy either.

When people do refer abuse to us, it's typically spam or phishing. We also receive from industry sources notices about malware.

So, when we get a actual allegation of true abuse, what -- typically, what we do is first thing is pass that along to the registrar. And we do that because, one, we're sensitive to the relationship that a registrar has with its customer. And, two, give the registrar an opportunity to reach out directly to the registrant and try and, you know, if there's a legitimate explanation as to why we're mistaken in our conclusion that something is spam, we'll certainly listen to it.

So registrars often do act on the referrals we send them and suspend the domains. But we always -- when we refer to registrars, we say in the event you don't act satisfactorily, we're going to take action under our anti-abuse policy. And, when we do, we suspend the domain. And, typically, we suspend the domain because deletions have proven pretty ineffective. Once

a domain name is deleted, typically, the very next day it's registered by the same individual for the same abusive purpose.

When we get referrals from law enforcement, they always receive the utmost attention from PIR. We work very closely with law enforcement, especially in helping to even craft language for potential orders so that the court can order exactly what a registry can or cannot do.

We also implement proactive measures to mitigate abuse of the DNS. And this is one area that we particularly work closely with our backend provider, Afilias. We have systems in place to flag unusual registration patterns. For instance, if a registrar has a substantial spike in their daily registrations, that gives us reason to look into their registrations. It doesn't mean that the registrations are necessarily abuse. Hopefully, it was just a good day. But it gives us good reason to look a little closer and conduct an investigation as to whether or not the domains might be spam.

Spam or other sorts of abuse.

We also get a report every day on the prior day's registrations. And we will cross reference the WHOIS information with various blacklists. Again, that doesn't mean that -- in case there's a match, that doesn't mean that there's necessarily abuse going on. But what it does mean is it gives us reason to look into the

registrations and see if something fishy is going on. No pun intended, by the way.

In the event we do find possible or likely abuse by these proactive measures, we generally follow the same steps that we follow for reactive measures. We reach out to the registrar, give them the opportunity to address or reach out to the registrant. And, if they do not act, then we do. We'll suspend the domain names.

And, with that, I will hand it over to Statton.

STATTON HAMMOCK: Namaste, everyone. Thank you for joining. My name is Statton Hammock with Rightside. For those of you unfamiliar with Rightside, it's a vertically integrated domain name services company, which means we're both a registry and a registrar. We're the registry operator for 40 of our own top-level domain names. And we're one of the largest registrars as well selling domain names of all types.

And so, as vice president of policy and business and legal affairs, I have a unique window on a lot of different abuse-related data that comes in both from the registrar side and from the registry side. And it's my pleasure to give you -- share some of that data

with you so you get a picture of what we're seeing on a daily basis, particularly with respect to new gTLDs.

But, first, when I talk about abuse, I want to be clear that when I talk about anti-abuse efforts, I'm talking about a number of different things, some of which are required by registries pursuant to the terms of our agreement with ICANN. And these are the implementation of rights protection mechanisms that have been -- that work designed, developed during the genesis of the new gTLD program. And these include the sunrise period, the claims period, URS and UDRP and sunrise dispute resolution process as well as a few others. And also, as a registry, we had to include certain public interest commitments that were baked in -- that were required. Some of these came from the multistakeholder community. Some came from advice from the GAC and other places. And those were also implemented into our registry agreements.

And then there's what I term the more voluntary or industry-led efforts that are not contractually required that registries and registrars have undertaken by themselves to combat nefarious activity on the Internet.

So a number of registries, including Rightside, offered a domains protected mark list or a block list to protect rights holders, intellectual property trademark owners, from having to spend

sums of money on all the different TLDs. Claims plus process where we extend the claims notice period longer than the required 90-day period to alert trademark owners of any registrations that may infringe their marks. And then other efforts include working on creating a security framework, which members of the registry stakeholder group are working on now to define some ways and processes we address abuse.

And then there's things that are far outside even these voluntary efforts within the ICANN community which are initiatives driven by individual registries and registrars to help curb different forms of abuse.

Working with some of these groups to take down child abuse internationally, some copyright content. There is the healthy domains initiative through the domain name association, which is the trade association representing the domain name industry, working on best practices and principles for addressing things like illegal pharmacies, security attacks, and other forms of abuse. So that's the landscape of anti-abuse efforts.

So from the Rightside side of things, we have over a million -- or over half a million registered domain names in our 40 TLDs. We have three abuse report sources that we use to monitor on a daily basis. We have three highly regulated top-level domain names. When I say "highly regulates" those are names deemed

to be highly sensitive by the GAC. These are .LAWYER, .ATTORNEY, and. DENTIST, these professional domain names.

We had zero public interest commitments disputes. Disputes are claims made against our 40 TLDs, zero sunrise dispute resolution procedures, and 52 URS proceedings initiated. So, while the data here at Rightside isn't necessarily indicative of the activity in all the registries, we see this consistent with what ICANN compliance is reporting out to us in terms of -- in terms of abuse. Sorry.

Most of it being phishing, malware and spam, which we expected to see. But very little on the content side or any of the other complaints that we had thought might be the case in new top-level domain names. Some are registry -- in response to these complaints, some of them are taken -- are actions taken by the registry, some by the registrar.

And finally, again, just to reiterate, you know, given the number of domain names that we're seeing registered now, a low level of abuse is being reported.

And this last slide shows the Rightside and my colleague Brian's TLDs here that we decided to share with you all. So thank you very much for listening.

BOBBY FLAIM: Thank you, Statton and Brian. I just wanted to ask you one question collectively based on what Drew asked. You guys collectively share information that you may have on abuse? Like, if you see particular actors or trends, do you share that information?

STATTON HAMMOCK: Yes, we do informally. This is Statton Hammock from Rightside. So at both the registrar -- mostly at the registrar level, my compliance team is willing to share with other registrars information they see from bad actors, right? If we see a known bad actor who is trying to hijack names or engaging in any other nefarious activities, we may share that information across different registrars so that they're aware of the same bad actor.

But nothing formal or required. But we do that as a matter of good practice.

BOBBY FLAIM: Okay. Thank you, Statton. Next up we have Giovanni Seppia -- sorry.

Sorry. The configuration, I can't see everybody. I apologize. Yes, question?

UNIDENTIFIED SPEAKER: Hi, this is (saying name) ICANN fellow, and I'm also NomCom 2 committee member. I had a question about various blacklists sources that appear from -- I have a question from PIR. You mentioned you scan your reports through various blacklist sources. Where do you gather those sources, and how do you do it? I'm sorry.

BRIAN CIMBOLIC: Sure. Thank you for the question. A lot of lists are publicly available lists, and a lot are subscription based lists. And often times there's some sensitivity around those lists, which some of their methods and whatnot. One of the reasons -- one of the ways we try to mitigate any possible issues with that is by the referral path that we by referring the registrar with the explicit request that they reach out to the registrant. So, if the registrant believes they were improperly listed, they have the opportunity to say why our conclusion that something was abuse is wrong.

I'm going to assume that these lists are -- that you source are generally verified or not just available on the Internet.

BRIAN CIMBOLIC: Sure. A couple of the top ones are SpamHaus and Serbil (phonetic) just to give you examples.

BOBBY FLAIM: Okay. We'll just take this one question. But I think what we may do is just, if we have questions, maybe just save them until all the -- you know, the end of the presentations. And that way we make sure we have enough time for the presentations. And I think we have allotted about 30 or 45 minutes for discussion or questions.

Yes, ma'am.

KIRAN MALANCHARUVIL: Thanks, Bobby. Kiran Malancharuvil from MarkMonitor.

As a brand protection company that summits a lot of abuse reports, I'm not in love with this graphic. And let me tell you why just very quickly. I think that it's not necessarily fair to say that, just because we're not reporting abuse, that there isn't necessarily abuse to be reported or that we're not reporting it elsewhere. Because of the fact that you have sort of very narrow abuse policies and you are very strict in how you interpret abuse, we've sort of learned as a brand protection company -- and I don't think that we're alone in our industry -- not to submit abuse complaints to you. I think probably a better graphic would be to help us understand how many domain names are being reported through all channels to ICANN compliance to registrars, to ISPs that are associated with your registry.

And I think that would be much better data for us to have when we're understanding what kind of abuse is being reported, not just what's being reported to you as a registry.

STATTON HAMMOCK: Thanks, Kiran. This is Statton with Rightside. The data that I'm showing shows abuse reports coming from all sources, including ICANN. It's coming from -- anything we get through the registry directly through our abuse Web site or coming from ICANN compliance is reflected there.

BOBBY FLAIM: Thank you. We'll just go straight to Giovanni.

GIOVANNI SEPPIA: Thank you, Bobby. Thank you for this opportunity. So I'm Giovanni Seppia, we're from manager at .EURid registry operator. And the first slide is to highlight ---

... As it's quite important us to underline our multilingual, let's say, aspect.

So we have implemented the series of measures to protect our domain names from an administrative perspective. So we have DNSSEC, the registry lock, homoglyph bundling which is a feature we launched a couple of years ago to make sure that IDN

domain names, whenever they're registered, if there are domain names that look like they are bundled, and, therefore, they are reserved, so it's not possible to register domain name that look alike, and in that way we protect those holders of domain names from possible issues coming from domain names that look alike and may be registered by other registrants.

And we also, as we have launched the dot in Cyrillic, we have implemented launched the script matching policy, so we only allow have only Cyrillic dot Cyrillic or Latin dot Latin domain names. And again, that is an extra level of security around the .EU environment.

Now, what we have implemented a couple of years ago is what we call the WHOIS quality plan. The authority of the .EU registry manager is very much limited by these two regulations, and, therefore, we have to operate thinking about what we can do in the framework of those two regulations.

We usually take action when we receive complaints about possible abuses linked to the .EU domain names, and most of the time we have great cooperation with our registrars, accredited registrars, and as a matter of fact, the WHOIS quality plan has been developed in close cooperation with our registrar and including the Registrar Advisory Board that provided EURid with great advice how to develop this WHOIS quality plan.

So what we do, we verify the registration data and we verify this registration data on a daily basis. And the registration data are verified either directly by EURid or upon request of third parties, some of them law enforcement authorities.

The main check relate to the address verification. As .EU domain name can be registered only by residents in 31 countries. And the address verification is done against third-party databases or Google maps.

Just to give you some statistics, at the end of 2015, we deleted more than 30,000 .EU domain names because they were not complying with the residency criteria set in the two regulations.

This is a list of many authorities. Belgium based or like the CERT-EU. We have a Memorandum of Understanding with which we have great cooperation and a dialogue. And as some of my colleagues in this panel were highlighting, it's a lot of education to make them understand what we can do in the framework of our regulation, of our public-policy rules, and how they can act in cooperation with us or in cooperation with our network of accredited registrars.

And the next frontier is the abuse prevention early warning system which we are currently developing. It's a quite interesting, let's say, analysis that we are currently developing in cooperation with the (saying name) University, and it aims to

predict possible abuses. And, therefore, to delay the delegation of registration requests for those domain names, again, that may lead to abuses.

Again, it's still in its infancy. It's a project that we have started about one year ago. And we are looking into that to make sure that, again, we can apply the prevention principle rather than fixing afterwards.

I'm happy to answer any question.

Thank you.

BOBBY FLAIM: Thank you, Giovanni. I have a question for you. It looks like you're doing a lot of anti-abuse and abuse mitigation. How -- Is it possible to quantify the resources that you deploy to do what you're doing?

GIOVANNI SEPPIA: Yeah, it's a good question, because what we have seen over the years is that we have decided some years ago to have the .EU and present and promote the .EU as a quality domain name. So we have invested more and more resources to profile .EU as a quality domain name which includes everything that we are doing to abuse mitigation and abuse prevention.

So in terms of resources, our legal department is currently staffed by three people that will soon be four, and two of them are mostly fully dedicated to the WHOIS verification, the WHOIS quality plan, and there is also my team, I am the external relations manager, my team is covering almost all European Union countries. And they do help the legal team in liaising with registrars. And what I would like to underline is the importance for registries to have great cooperation with registrars.

And we have had great examples in the past year of actions taken by our accredited registrars against some of their resellers who were abusing the system in our case. And some actions led to determination of the contract between the reseller and the registrar because the reseller again was abusing the entire registration system.

So again, I think that's a key element in this abuse fight and prevention.

BOBBY FLAIM: Can I just ask you a follow-up question since you mentioned you work effectively with the registrars?

How specifically do you do that? Are you seeing things that trigger -- trigger something that you need to go to the registrar? And how do you do that?

GIOVANNI SEPPIA: So whenever we see (indiscernible) attacked a domain name with registration data -- namely, the address or name of the registrant or other data relating to the registrant that are quite suspicious, we send an email to the registrant, to the email address that was provided at the time of the registration, and we always copy the registrar.

And most of the times, before deleting a domain name, we, let's say, liaise with the registrar to make sure that also the registrar is given an opportunity to liaise with the registrant as they are, of course, the channel for the .EU registrations.

And most of the times, as I said in the past, some of them were a bit reluctant because that was meaning to them an extra burden because it was extra resources that they are under. But now again I can only report a great cooperation with all our registrars. So I cannot report one single registrar who has not helped us in this kind of WHOIS quality data plan.

BOBBY FLAIM: Okay. Thank you, Giovanni. We'll just go straight to Michele.

MICHELE NEYLON: Thanks, Bobby. Michele Neylon.

So I'm Michele Neylon, a registrar, we're also a hosting provider.

So I'm going to speak kind of briefly to some of the -- some of the challenges that registrars and other service providers face.

Others have talked about some of the data that they -- that they have, some of the challenges that they face. So from our end as registrars, and also, you know, hosting providers, ISPs and others, one of the biggest issues we face is in relation to the reports themselves.

So over the last couple of years, there's been a number of initiatives in various different parts of the kind of broader security and anti-abuse community to try to improve the overall quality of reporting. But we're not quite there yet. I mean, as others have said, there's no real standards out there at the moment. Some people would complain -- would complain that there's no standards in terms of the responses, either.

So just a couple of very simple take-aways for any of you who want to report things to any of us. Just reporting, you know, what the actual type of abuse is that you think you're seeing. Providing us with clear examples of the abuse.

I mean, I looked at our abuse desk earlier today, and there was -- and the report simply said domain X is involved in abuse. That's super helpful. You know, I'm going to have to work out exactly what kind of abuse had a is. Abuse how? I mean, I don't know.

You know, the other thing as well, when we're talking about abuse, on this session, looking at it in terms of keeping that scope narrow. From a registrar perspective or speaking as a hosting provider, we're not going -- we do not want to end up in a situation where somebody is asking us to act as judge, jury, and executioner. We need to be given clear guidance as to what the actual complaint is, why it falls within our remit to deal with it, and, you know, what you expect us to do about it.

In the case of, you know, malware, botnets, all of those kind of things, I think generally speaking, most of us have no interest in having that kind of content on the domain names that are related to us. Domain names, however, if we are just acting as a registrar, we don't have a fine tool.

I can pull the domain completely. I cannot pull parts of a domain.

I can take it away and kill it completely, which would kill all services associated with it.

So just making sure people understand what you're asking us to do. Understanding what we can do, understanding the limits around -- around that.

I mean, here at this meeting, there's quite a bit of talk around some of the reviews that are ongoing. And I see members of the

CCTRT are here; that they are putting -- they are doing a review which includes abuse. And they will hopefully be able to bring us some concrete data.

And it's data that helpful for us. I mean, is there a relationship, for example, between domain names of a -- in particular extensions and their usage? Is there relationship between pricing strategies? But actual data would be helpful rather than just theories.

The other thing as well is that, you know, ultimately, as registrars, we -- we want to work with the rest of the community, but you have to understand that we are limited in what we can do. And if we're asking you for more details, it's not because we're trying to be difficult. We're just trying to understand what it is you want to complain about or what the issue is. I don't have a huge amount more to say on that.

I mean ultimately, from our perspective, I think it's down to the quality of the reports themselves. If the community can work on improving those reports, that would help us all move forward to something a bit more positive.

Thanks.

BOBBY FLAIM: Michele, I just want to ask you a follow-up question. You said when you're given the specificity to act on. Do you have any examples insofar as maybe an operational security company or a particular constituency that provides that kind of needed specificity that allows you to act?

MICHELE NEYLON: Sure, Bobby. That's a perfectly good question.

I mean, for example, in the case of law enforcement, you might want us to preserve logs if we're hosting -- hosting the domain name. Or if we're just acting as the registrar you might want us to take some other kind of action apart from deleting or suspending the DNS.

It depends, obviously, a case-by-case. But I think the real thing is it's more of a -- rather than saying to us there's a problem, it's a case of there's a problem and we would like you to do this, this, and this.

Now, for example, a common issue, and I think others may have touched on it, is around jurisdiction. My company is Irish. You are U.S. law enforcement, and much as we love each other dearly, if you send me something under U.S. law I will politely but firmly tell you to get lost.

Now, if you send it to me under something which I can act on, then that's fine. But if you send me something, say, for example, common one I always give you is DMCA. As an Irish company, not only am I not bound by the DMCA but legally speaking I cannot act on the DMCA. Now, that doesn't mean I'm going to ignore the report I'm giving you, but expecting me to act on it directly is not going to happen.

So it's down to, in some other realms -- Bertrand De La Chapelle's Internet jurisdiction project, he's been working on some of these templates around, you know, reports. So things like the jurisdiction comes in there; you know, what the actual legislation is; and, again, you know, the expected action.

It's just the more specific the report, the easier it is for us to make a determination as to whether we have enough information to take action or we need to put it back to you saying, okay, this is beautiful but you're not in our jurisdiction or you haven't given us enough detail to do anything about it.

BOBBY FLAIM: Thank you, Michele. I know that is a big issue when we're talking about DNS abuse, since we're not under international treaties, international crime conventions concerning the DNS. So when we're talking about conflicts of laws and, of course, the complicated legal system, I know in the United States we use the

MLAT, the Mutual Legal Assistance Treaty, and sometimes that is not optimal It takes a long time.

So those concerns are very real and they do present very specific challenges.

So can we just hold the question? I just want to get Denise in, and then she is our last presenter, and then we could take all the questions that everyone has, if that's okay.

DENISE MICHEL: Thank you, Bobby.

So I'm going to highlight the challenges that businesses worldwide and their users and customers face.

So few companies have the same scale and adversaries as Facebook and its family of companies. We do a great deal to protect our users and also help secure the Internet.

Domain names are both a source of abuse and are key to detection, deterrents, protections on our global platforms. A single malicious domain name spawns numerous FQDNs, and this is a point that is often overlooked or perhaps many in the ICANN community are not aware of this.

So a fully qualified domain name is the complete domain name. That's the host name and the domain name.

So a single malicious domain name spawns numerous FQDNs that in turn spawn an exponential number of URLs. And our platform, and businesses worldwide, then, end up with several orders of magnitude of badness or harm to our users as a result of one single malicious domain.

So I have a whole number of slides on -- that are posted on the session page and reference a number of key elements of both the RAA and the RA; tools that can be used and contractual obligations to help mitigate abuse.

So of course the registrars and registries can and do play a gating, a mitigating function in relation to DNS abuse and have contractual obligations to do so that are indicated in these slides.

They should also have a business incentive to do so because protecting the end user is good for protecting the DNS ecosystem and the domain name registration business.

I'd like to highlight a real-life example of how this plays out.

Two domain names a few months ago were registered. Com-video.net and login-account.net. They were registered using Facebook's complete name and contact details. Here is the WHOIS record for Facebook.com. Hopefully you can read that.

This WHOIS record, all the information in it, was taken and used to register those two domain names.

As you can see here, it's all Facebook's information, including our email address, except for the name servers.

So these two domain names were then used to launch phishing malware abusive attacks against about 30,000 users. The scheme was quickly detected by Facebook and blocked and immediately reported to the registrar, onlineNIC and also to the ICANN complains team.

Now, the registrar did not verify the registration of these two domain names using the registrant's email address, which was us. We immediately filed a complaint after contacting -- trying to contact the registrar multiple times. We filed a complaint with ICANN compliance, which was opened and then closed within 24 hours with absolutely no change to either domain names or the WHOIS record.

Ultimately it took two months and dozens of communications to cancel two domain names. This is despite the registrar's acknowledgment -- the registrar's acknowledgments that the WHOIS record was fraudulent and the domains were used for fraudulent purposes.

So the lessons learned from just this one real-life example is that the system fails if a registrar doesn't do the basic verification at the point of registration. The system fails if a registrar is inattentive to abuse reports. The system fails if the registrar is unwilling to take appropriate remedial actions afforded under the RAA. And in this instance, onlineNIC insisted on obtaining the account holder's approval to modify the WHOIS. This is the same account holder who perpetuated the fraudulent registrations and use of the domains for fraudulent purposes. You just can't make this up.

And the system fails if ICANN compliance closes the ticket without results and then takes, quote-unquote, "cooperative enforcement efforts" with a registrar who is noncompliant.

So as a global platform, Facebook certainly understands that not everything gets caught at the gate, and abuse prevention procedures are not perfect. But our community should demand that. All parties employ good faith efforts to follow existing abuse prevention policies and procedures; that when procedural failures are identified, that they are rectified promptly. For example, it shouldn't take over two months to address blatant false WHOIS tied to fraudulently used domains. And ICANN needs to address ignored or habitual system procedural failures through appropriate contract compliance.

So we don't have to recreate the wheel. Abuse prevention policies and contractual obligations already exist, and are used appropriately by a majority of registrars and registries, some of them sitting at the table. We need to implement them across the board.

Thank you.

BOBBY FLAIM: Okay. Thank you, Denise. We have about 12 minutes for questions. So I just wanted to -- I know, Peter. Apologies, but you're the first up, so I know you had a question. So if anyone else has questions, please feel free. We have until 3:00. So thank you.

PETER VAN ROSTE: Thank you, Bobby.

Good afternoon, everyone. My name is Peter Van Roste. I'm the general manager of CENTR, and CENTR is the organization for and by European ccTLDs.

I wanted to answer a point that Michele raised; that is that there seems to be a lack of understanding of the different factors in what will increase or decrease the abuse in specific domains.

We have done a study at CENTR about a year ago. There is a high-level summary of that that is available, will be tweeted to you shortly. So feel free to share.

And in addition, I know that some CENTR members have done in detailed research on specific factors. I have no idea whether that information is already public, but I'm -- I know that they have the intention to make that public any time now. That's one thing. So hopefully that represents.

Secondly, crucial for this discussion, I think for Europeans, is the discussion that has been taking place in the framework of the digital single market. And there, under a consumer protection review regulation, the proposal is to help solve or help protect European consumers by closing down domains, by temporary disabling access to content, et cetera.

And the recurring problem there, and which is something personally I found quite confusing in this panel, too, is the lack of common vocabulary to define what we're talking about. And especially towards governments, law enforcements in Europe, you feel that there is a need to start harmonizing that, and I would suggest it to this panel to see if there is any opportunity to, as a larger community, not just us European ccTLDs, but as a larger community to tackle this problem.

It's not an easy one, but it is something we will need to address sooner or later.

Thank you.

Thank you. Mike?

BOBBY FLAIM: Does anyone have any comments on that or -- Michele, go ahead.

MICHELE NEYLON: Thank you. Michele Neylon, for the record. That's a very helpful piece around the statistics and data. The problem, of course, is I'm speaking in relation primarily to do with gTLDs, not Cs. But thanks. And I am 100% -- before anybody says it, I'm 100% agree that it's Cs and Gs. They're all just domains.

BOBBY FLAIM: Thank you. Mike.

MICHAEL PALAGE: Quick question to Allen. Does ICANN compliance get any type of regular abuse reports provided by third parties as part of their assessment of abuse and registrar compliance?

ALLEN GROGAN: You're thinking of abuse reporters like SpamHaus or those kinds of commercial reporters?

MICHAEL PALAGE: I'm asking because I did a recent DIDP request trying to identify what sources ICANN is undertaking. And it was rather lacking. So I'm just trying to see does compliance get any reports? ICANN was rather cryptic claiming confidentiality and other stuff. So I'm just trying to ascertain what resources is ICANN staff, security teams providing your team to do its job?

ALLEN GROGAN: So I'm not sure I can authoritatively answer that. ICANN compliance I don't think routinely uses third party sources. I think the SSR team probably does refer to those things. Carlos, can you address that?

CARLOS ALVAREZ: You're talking about when someone reports an abuse they feel they didn't act reasonably and then come to ICANN compliance and file a report?

MIKE PALAGE: What I'm trying to gather is I think it was yesterday Margie in the CC group was talking about how they're going to try to

undertake an analysis of abuse from legacy gTLDs to the current marketplace. So, if they're undertaking this historical analysis versus what was in the past and what's today, where are those data points being collected? In order to do that, someone must have collected that data.

CARLOS ALVAREZ: I think the right question would be to ask the ccTLD to see what their methodology looks like and what sources of information they're looking.

MICHAEL PALAGE: So what does the SSR team -- what do you do? Can you share what reports you run? Or what do you do to do your job and then what do you share with compliance? Or are you just operating in silos? I guess that's what the question is. Is there communication?

CARLOS ALVAREZ: We don't produce reports of abuse. That's not our job.

MICHAEL PALAGE: Okay.

CARLOS ALVAREZ: We do analyze data regarding abuse. We do identify registrars that might be registering large numbers of domains that might be considered malicious. And, when warranted, we share the information with the compliance team for them to address within their process.

MICHAEL PALAGE: Okay.

BOBBY FLAIM: Mike, maybe you could take it offline with Carlos after.

MICHAEL PALAGE: Yeah.

BOBBY FLAIM: Okay. Sorry. We have just a few minutes, so I guess we'll just end the line here. Kiran, please.

KIRAN MALANCHARUVIL: Thanks. Kiran Malancharuvil from MarkMonitor again. First of all, really great session. So thanks, everybody. I'd like to hear what Mr. Grogan's response was to the concerns that were raised by Denise Michel from Facebook.

Fraudulent WHOIS records is a big issue. MarkMonitor and a group of brand owners recently submitted to ICANN a report which contained thousands of domain names that were registered in dot feedback with WHOIS records that have been stripped from corresponding dot coms that mirrored brand contact information in the same way as the example that Facebook provided for you in her presentation today. So I would like to hear what Mr. Grogan has to say about the concerns that Denise raised about how compliance is dealing with those reports.

ALLEN GROGAN: So I'd say two things in response. One is we don't generally address individual cases in public forums regarding compliance matters.

And the second thing is I'm just not -- I was not prepared to discuss this. I have not reviewed either this or the MarkMonitor complaints in preparation for this session. And I'm not in a position to address it now.

KIRAN MALANCHARUVIL: So you've never seen fraudulent WHOIS before we blindsided you with the event in this forum?

ALLEN GROGAN: That's not what I said, and that was not the question. You asked me to address the specific complaints that Denise made. And I did not prepare to do that in preparation for this session.

KIRAN MALANCHARUVIL: Thanks.

Okay. I thank the panel for the -- my question and comment is to Denise. You are speaking about the two domain names which were posting fraudulent WHOIS information. And you said it took almost two months to take it down by the registrar.

So, first of all, I just wanted to say I represent dot industry. The dot industry indeed we have more than 100 registrars. So in cases where any complaint comes to the registrars who are not registrars, they are given some time limit to take action on that. In case they don't take action within 48 hours or so, they go to the registry so the registry start to take action within 42 hours given we take action. So why not -- we're just trying to ask you that why didn't you write to the registry? Concerned registry of the domain names and write -- why wait for two months? Indeed, exactly.

DENISE MICHEL: So we contacted the registrar directly, the registrar that was responsible for registering the domain to try and get that

registrar to fulfill its obligations under the RAA and to have the domain that had all of our information actually put under our control. And then we involved ICANN compliance as it is their responsibility to deal with complaints in terms of the registrar fulfilling its obligations under the RAA. So this is the process and the contractual obligations provided for registrars. And it was important for us to follow the procedures and obligations that are laid out by ICANN and its contractual -- it's contracts with the registrars. We understand that of course the registries -- and I highlighted some in my slides -- also have some responsibilities. It is so prevalent in some registrars, this type of behavior, that we felt it was important to get a full record and accounting for just how long it would take in this process to pull down these two domains.

I just have a word still, can I say? Okay. But I slightly disagree with you in the sense that you have to go for ICANN complaints committee or something like that you are to contact. But here level registry, registrar, registrant. The registrar not taking action I think you should have gone to the registry level. I think that would have easily solved the problem within a week or so.

MICHELE NEYLON: Just to respond to the gentlemen there. Michele speaking, very briefly. I believe Denise is talking about dot com names. And, as

such, the registry does not have the WHOIS data for the domains. Now, maybe complaining to the registry, the registry, if they keep getting complaints, will probably get a bit upset with the registrar and send something back to them. But for dot com and dot net, the registrar is the one that controls the WHOIS data. And there is only the registrar can make changes to the WHOIS data. I'm not trying to defend any registrar specifically. But just in terms of that relationship. If it was a thick registry, as is the case for dot.org or any of the Rightside TLDs, then I think the relationship would be slightly different. But when we're talking about common net, the WHOIS data resides at the registrar level only, not the registry.

I was just trying to say that there's agreement between the registry and registrar in case of registrar not acting. And the registry can take action.

MICHELE NEYLON: If you want to take that offline, that's fine. BOBBY FLAIM: Maybe we could do that. We just have a couple more questions, we're just supposed to end, so thank you.

PAUL McGRADY: Paul McGrady. I don't know what hat I have on, maybe my author's hat. But the effort -- for 15 years I've only had

something similar to what Denise is talking about happen to me. And I thought well, I'll just ignore it. Once every 15 years means maybe I've got one more. But we had something very similar happen where we think it was an upset loser of a UDRP complaint register a bunch of domain names that contained the client's perfect information and ours. Essentially the same information that would follow UDRP complaint. And we wrote in to the false WHOIS complaint. The registrar who was not based in the U.S. suspended the domain names instead of deleting them. And we were told by ICANN that, once the domain name is suspended, it's not considered to be a real domain name any more and that was just the policy and practice. And I just think that, of course, then you've got to watch it, make sure it's not unsuspended every single day and then you have to watch them to drop. And you're just adding cost and aggravation into the system. So, again, if that really is the practice, I think it's quirky. And it sounds like it's from a prior happier time in the Internet.

And so that might be one little gap that ICANN wants to track down and see if they can figure out how that ends up not being the outcome. Because that's -- when you've got the people in the WHOIS record saying it's not us, then I think that that's -- you know, that's a pretty straightforward situation. Thanks.

BOBBY FLAIM: Okay. Last question, Nick.

NICK SHOREY: Thanks Bobby. Nick Shorey from the U.K. government here. I'd just like to say I think this has been a really great discussion, so thanks very much for setting this up and to everyone on the panel. I think there have been some really interesting ideas as well that we can maybe look to take forward over the coming months around sort of collaboration, how we can improve public safety requests when they're making them that Michele spoke about there. And it seems to me, within this discussion, yes, there needs to be some work on defining what we mean when we say -- when we talk about abuse. And that definitely needs to happen would be advantageous.

And also there's a distinction between proactive and reactive responses to abuse. So a lot of the stuff we're talking about with regards to improvements to WHOIS validation, that, ultimately, is like a proactive action. And then we've got reactive. I would be interested to hear, as a lay techie, whether a registry sees the entire URL, for instance, when a DNS request is made. If they see all that information, that gives them a huge amount in terms of cybercrime space, potentially, huge amount of insight on sort of a particular piece of malware, and if there's a spike in traffic going towards that. So I'd be interested to see if they know that.

And I think maybe next time -- because I do think we should do this again -- it would be really great if we could get, like, a network operator here and, like, a hosting company. ICANN's always engaged in this difficult debate around, you know, we don't -- we're not a content regulator and et cetera, et cetera. I can appreciate that standpoint.

So I think it would be good to sort of understand that collaboration and maybe get someone who does purely hosting or a network operator to just broaden this debate. So thank you very much. Cheers.

BOBBY FLAIM: Thank you, Nick. I think that actually is a very good idea about having the hosting providers and network operators. Michele.

MICHELE NEYLON: Thanks. Nick, I'm all three. I'm a network operator, a hosting provider, and a registrar. So you get a bit more bang for your buck.

In terms of the DNS request query about URLs, I think we need to sit down and I'll explain to you more about how DNS servers work. The registry wouldn't see that. The registry will know which name servers a domain name is using, but they will not see every single DNS -- sorry. They will not see any DNS requests

for a domain name in the registry, essentially. They'll -- they see the other level to do with the tiers. But happy to go through any of that if you need help. Thanks.

CARLOS ALVAREZ: This is Carlos from ICANN SSR team. I want to say one more thing, because we're over time already. There are over 2,000 or around 2,000 registrars, and those that we have decided to look into are very few. Very, very few that are actually worth looking into with regards to malware, botnet control, or phishing.

That's within ICANN's remit. There's a lot of comments in the operation security community with regards to registrars that people may see domains used for spam. Spam is not within ICANN's scope. It's not mentioned in the GAC advice provided in April of 2013.

It's not mentioned in the -- in spec 11, so we can't address that. We can't look into those registrars. And, when we decide to review a registrar for any particular reason and we pass it into compliance, compliance does their work. And, if they find that the raise was compliant, there's little else to do. So what I want to bring here is that it's really more up to the community to address this issue, if the community so thinks that it's worth addressing. But we get the tomatoes. But it's something that

the community needs to address and discuss from the security standpoint. Thank you.

ALLEN GROGAN: Just real quickly -- I know we're over time. As I said, I didn't come prepared to address the particular case that Denise raised. But my team in the meanwhile messaged me. Just to be clear on the facts there, the domain names were suspended on the first abuse report and remained suspended for the entire two months. So it's important to get that context there. Thank you.

BOBBY FLAIM: Giovanni has one last comment, and then we're going to have Alice wrap it up.

GIOVANNI SEPPIA: Thank you, Bobby. Just that I believe that today's discussion, this very short session highlighted how much it's important to have education, cooperation, and dialogue among all the stakeholders. It's not a matter -- when speaking about abuse, it's not a matter of pointing the finger at any of the parties involved. Just a matter of communicating and making sure that there is a common understanding of what we can do together. Thank you.

DENISE MICHEL: In that spirit, I mean, it's important to understand that a fraudulent WHOIS on a domain name that's being used to attack users on the Internet and has my company's information on it, should not remain in the public domain in suspension.

And I have no doubt that if Knightside had been the registrar or -- I mean, Michele's company Blacknight or Rightside, these registrations would have been verified with email. And, if that had somehow slipped through, it would have been 24 hours and they would be down. Completely.

Suspended is not a resolution in this case. And, you know, we raise this as an issue. This is not unique. We have a lot of challenges in this area. And, you know, I want to underscore the fact that, you know, compliance -- I'm really happy that compliance is getting priority from the new CEO. And it's a critical issue in our fight with abuse. Thanks.

ALICE MUNYUA: Thank you very much. First I'd like to thank the panelists for the great informative presentations and most of all for keeping time. We were very tight. And to thank you all for the great discussions and questions. And I know you had much more questions. So the panelists had prepared much more detailed

presentations. So, for those interested in getting to understand more on some of the topics that were presented today, we'll have the presentations online.

I'd like to thank Bobby for moderating the session and Fabien for organizing it.

We're now going to the next PSWG high interest topic discussion on WHOIS in five minutes. Thank you.

(Applause.)

[END OF TRANSCRIPTION]