TERRI AGNEW: Good morning, good afternoon, and good evening. Welcome to the At-Large capacity building program 2015, fifth webinar on the topic of understanding and distinguishing among cyber activities, taking place on Wednesday, the 15th of April, 2015 at 21:00 UTC.

We will not be doing a roll call, as it is a webinar. But if I could please remind everyone on the phone bridge, as well as computer, to mute your speakers and microphones, as well as state your name when speaking, not only for transcription purposes, but to allow our interpreters to identify you on other language channels.

We have Spanish and French interpretation.

Thank you for joining, and I'll now turn it back over to our moderator, Alan Greenberg.

ALAN GREENBERG: Thank you very much, and I'll note that I am replacing Tijani Ben Jemaa, who is out of town at the moment and couldn't participate. But I have to give full credit to him for being the organizer of these webinars. We have what I think is going to be an interesting talk today. It's a little different than our normal ones, in that many of our normal ones focused quite closely on ICANN activities, or related to things that are going on in the ICANN sphere.

This one is a little bit more general. And I must admit, I did go through the slide deck, and I thought it looks pretty interesting. So I'm eager to

see how it turns out as well, as much as you are. And I'm intrigued by the fact that there are no capital letters in the title. And I'll turn this over to Steve Conte.

STEVE CONTE: Alan, thank you very much. And I have to admit that this is not my presentation, this is Dave [Fis-co-tello's] presentation, and he is unfortunately travelling on ICANN activities right now, so I said I would fill in for him. So any mistakes that are made, are mine alone. Dave is a much smarter gentlemen than I am, and I'll take all credit or blame as it falls.

A little bit about myself. I see the list here, and some of you I know, and some of you I don't. So let me just give you a little bit of background of myself. My name is Steve Conte. I originally started in ICANN in 2002, working as a system administrator, and eventually started… Back then, ICANN was very small so we wore many hats. I think I was employee number 13 or so.

And so I've done IP at ICANN, I've done IANA. For a period of time, I went back to IP, and was the general manager of IP for a while. And then I went to Chief Security Officer, before I took a leave at ICANN when I worked at the Internet Society for about five years. And then about a year ago, I came back and joined the Security, Stability, and Resiliency under John Crane.

And having a ball, glad I'm back. So glad to meet all the new faces here, and happy to see all of the old faces here. And let's get going on this.

I'm a very open presenter, so if you have any questions or comments, please, I've got the chat window open, I'll be watching that as well, or jump in on the call, and interrupt at any time. I've got no rhythm to this, so and I'll pick up from where I leave off there.

So today I want to talk about the understanding and the distinguishing among different cyber activities. And as Alan said, this is kind of a very high altitude presentation. And at the end, I am going to go and try to drawback on what parts relate to ICANN, and specifically, what parts relate to the SSR team in regards to, you know, what we look like and why we're looking at cyber activities, both legal and illicit activities.

So I'm not going to read the slide word for word, but as I just said, cyber is a very big word, and you know, it kind of relates to anything digital, and in this case, anything Internet related. It is difficult to put a tag on things, you know, news agencies, and news papers, and media will say cyber attacks. And it's such a large word. And we wanted to kind of talk about what a cyber activity is, how you can distinguish what type of cyber activity is taking place, and you know, make some conclusions on your own from there.

So we're going to look at three different models of cyber activities. We're going to look at the means, the motive, and the opportunity. And I'll dig into these in the next slides, but I'll pause here and hover for a second so you guys can take a look at the slide. We're talking about financial under means, we're talking about financial, technological, and intellectual, motive, different aims, political, business, financial, notoriety.

And opportunity is various access points to the Internet or from the Internet. So if we take a closer look at means in cyber activities, we're looking at ways that cyber activities must be funded and financed. You know, we're not just talking about criminal activities at this point. So there are many legitimate, more, hopefully, legitimate entities out on the Internet than there are the illegal activities, and they all need to be funded and financed somehow.

So a lot of means for cyber activities would go through and use the networks and the Internet to do that. Commercial, NGOs, government funding or financing, use cyber activities in order to pay for the digital goods, they're bound to use open source, or they're people underneath these organizations that are working for them as well.

And then of course, the criminal financing. You know, everyone gets at least 40,000 emails a day that say click here because Amazon just gave you a $15 gift card. Those are ways where the criminal activity is trying to get you to either subscribe to something and give them your credit card information, or attempts to hijack your computer, and that way they can either use it for watching and looking at your credentials and your data, but also using that computer for illicit activities.

And then there is activism. A lot of organizations use the Internet and their cyber activities to further their causes. And then a sub-note of that is "hactivism" which is normally a criminal means, and you'll see that in the form of a hacked website, because they're disputing an organization or other means.

If we take a closer look at opportunity, the Internet is open access, common technology infrastructure, as well, and we're part of ICANN, in the process. It does drive its [inaudible] from [add up to its adaptabilities?], excuse me. And you know, adaptability is great because it's showing us this nebulous, or this organic model that the Internet is. It constantly adapts to what we want it to be today.

I mean, if we look at this 20 years ago, we would be having, talk about gopher and possibly the new HTTP that was coming out at that point and stuff. So it adapts as we adapt, as we have more needs, it has more opportunities, and that's through organizations through IEPF and IEEE, ITUC. As we build new protocols based on the demand of the users, then the network adapts to what our needs are.

And that works both for legitimate and illegal activities as well. And then finally, we'll take a look at motive. So there was, on the different types of aims, we had protocol, we had commercial, we had… Protocol, business, financial, and notoriety for their different types of aims. So you can determine what an activity is based on the motive that's happening to.

So political aim, we've all see, I'm sure, some kinds of emails, or websites, that are promoting, or furthering, some kind of political agenda. Same with business agenda. In fact, political agenda and the business agenda kind of blurred together if you look at Net Neutrality and all the work that took place around that subject.

And I guess, in some ways, it would be commercial as well, that we're taking a look at that. The commercial could also be just having cookies on your web browser, and profiling you as an end user, or a consumer, is doing on the Internet. So, you know, a large search organization, either Google or Amazon as a provider, they have a better idea of what to target to sell you things, or provide you a more focused service.

Whether that's good or bad, that's really up for you, as an individual, to decide, whether or not you like that type of activity. So when we look at, as I look at these in general, we're going to go through a couple of different scenarios of the cyber activity. So we'll start with the cyber security. And all of these are 30,000 foot words. There is really no clear definition of what cyber security is, because there is so many facets to cyber security. And at the end of the presentation, we'll talk about the fact that ICANN's SSR team looks at cyber activities, with the IANA cyber security.

But this is [inaudible] practices of, to protect networks, computers, and I'm going to throw in devices too, because there are so many different mobile devices on the Internet now as well, cell phones and tablets and other types of devices that it's not just necessarily your laptop or your desktop.

So it's to protect these devices from, and the data within from digitally mediated attacks. And those attacks can fall into many different forms. They could be a phishing attack. They could be, you know, email, a fraudulent email. They could be a file that was downloaded on your computer that was clicked and suddenly the bad guy has access to your

computer or your device. There are so many different types of cyber security incidents.

One of which is a cyber attack. This is an online attack against digital or physical assets. Most of the time, these are against digital assets. I know, a number of years ago, there was an attack on Microsoft. This goes back maybe eight years ago. An attack on Microsoft, and the bad guy who attacked Microsoft used the root servers as a resource for them to attack. They would send a malformed query to a root server, and the root server would think that it's Microsoft that was asking, so it would respond to that website.

And so the bad guy sent a lot of little packets to the 13 plus root servers out there, and we sent a whole lot of data to Microsoft. And Microsoft called us up and said, "Hey, why are you attacking us?" We're not. So we looked into it, and sure enough, there were malformed packets coming in.

It's things like that where you're attacking, it's both the digital realm of the Internet, but you know, you could also use that to attack not necessarily a DDOS attack, but other methodologies to attack and slow down physical assets as well. There has been known attacks on ATM machines, as well.

Then we look at cyber crime. This is online activity that has been classified as a crime, or online activity that is committed in violation of the law. And these days, almost everything involves some sort of cyber crime component to it. When we worked with law enforcement, and

public safety organizations around the world, and they're looking at how to find whatever perpetrator they're chasing at that moment, a lot of activity has a cyber crime component.

And that could be something as simple as sending a SMS, or an email from one bad guy to another. Or it could be a complete online crime that is taking place, that could be, if someone is trying to steal your persona, and your ID, and do that, they might be doing that entirely through Internet or network means.

There is cyber warfare, and this is attacks on a nation state by a nation state. You don't hear a lot about this in the news, although there is a fair amount of it that does take place between nations. I don't have the insider information on that, but it does take place. And there is, I don't want to call them cyber armies, but there are individuals in every branch of military, around the world, not just in the US or in other countries, but around the world that work on mostly mitigating cyber attacks.

And this is actually an interesting point, because they haven't determined whether an attack is coming to a military installation via a server at the Department of Justice, or something else around there. They have to determine, or try to determine, whether or not that attack is coming from an individual, a non-government group, or a government itself. And it's sometimes, oftentimes, very hard to determine where the, who the source of the attack is coming from.

As far as, you know, depending on what type of an attack a government maybe seeing, because a lot of times, or sometimes I should say, they might use an entity that's not affiliated with the government to produce that type of an attack on a legitimate government.

And then there is cyber terrorism. And as it says here, it is an immediate attack, an intimidation attack on a nation [inaudible] …by civilians to personalize war. Much like terrorism in real life, or in the physical world, it's all real life in some ways. This is mostly about a civilian to a civilian, or a group to a civilian, or a group to a company, but not necessarily a civilian to a government or military that would fall under normal criminal activities, unless or until, you know, if there is a hack and they're able to get state secrets, that could change things a little bit as well, but this is mostly about trying from one group of citizens trying to attack another group of citizens for political purposes.

And then we have cyber surveillance, sorry I can't talk today. This is a digitally mediated and covert information monitoring or collection. And this falls, this is another 30,000 foot word because this falls under, could fall under so many things. This could be as simple as cookies on your browser, because Amazon wants to see what you've been shopping for so they can give you better products, product suggestions.

This could be, you know, the famous Snowden and NSA stuff that takes place of governments looking and monitoring certain channels, or certain servers, or looking for certain keywords, and things like that. This could be me, at my house, making sure that my son doesn't go to the sites that I don't want him to go.

So I might have something installed on my network. There are so many levels of cyber surveillance that take place, that you really have to provide the context around what type of surveillance is happening, and what you're looking for, or what they're looking for in order, why they're having this surveillance on you or on your devices. And there is activism and "hacktivism."

This is protests against commercial or non-commercial entities, or nation states, or a group of individuals. This is hacked websites that you hear about on the news, or that you might have experienced in your company, or seen in other media where a group of, I'm sorry. I'm jumping right to "hacktivism," and I'll continue that and go back to activism.

Where a group of hackers, or script kiddies, or something like that, want to make a message. And typically, it's because somebody has angered them somehow either through product, through chat room, or something like that, and they want to make a statement. So they will hack the website through known issues with the web software. They'll hack those and compromise it, and then put a new webpage up.

And a lot of times this happens with news media, but it does happen on a personal level, to some extent, you know, if you're in the chat rooms and if you're making comments, or if you're leaving comments on a blog, or something like that, that might irritate someone enough that they might want to take action against you and show you that, you know, that they can do this and you have to kowtow to them.

When we look at activism, we're looking more at a legitimate organization trying to put their message out in a non illegal fashion. It could still be a fashion that you don't want to accept, or it could be unsolicited email to you, but that still would be an activist activity.

Spam, unfortunately, isn't illegal. It's just a minor annoyance, so a lot of organizations will use email as a medium for delivering their messaging. It's not entirely meant to, at that level, that's the activism level, it's not meant to become an attack of any kind. It's meant to have that organization further goal by providing awareness, or information, or just trying to get you to sway your opinion on that. And it rarely, if you're a legitimate activist organization on the Internet, you rarely move to an illegal mentality, because that would adversely affect the goal which you're trying to achieve.

And hand in hand, really, with the "hacktivism" is just vandalism. So vandalism is much like the "hacktivism" that I just spoke about, where someone will hack the website because they want to, they have a disagreement the mindset or the goals, or the organization, and they want to take over that website. But sometimes that kind of stuff just happens because hackers want to be known. And it's, they want to show the rest of the world, and especially their hacking peers, that they can do something.

So it's, you know, in California, we have a lot of vandalism, and graffiti, and stuff in the city, and on the walls and stuff, and we call that "tagging." In some ways, this is just a digital version of "tagging." It's to show that you as the bad guy, pending various definitions of bad guy.

You as a bad guy have come here and you're made your mark, and now people know that you can do this, or that you have done this.

And so they now they can go and they have bragging rights back in their circles of hackers, or criminals, or whatnot. I think I mention this in a prior slide, most activities are rarely exclusively cyber. There is always some kind of physical component to them, not just criminal activities, again, but physical activities too. Most activities, and if we look at activism as an example, very rarely would you have a solely cyber activist activity taking place.

It's usually in conjunction with something that you, as an organization, are doing from a somewhat physical perspective too, and you're just trying to use that as another channel to reach people. When we do talk about criminal activity, there is almost always a physical component to the criminal activity as well. They're looking to do something, or gain something, or if we're talking identity theft, there is going, they might use the Internet as a piece of gaining pieces of your identity, but they're going to turn around, at some point, and use that in the physical world to set up a demi-corporation, and try to borrow three billion dollars, or whatever it is.

There is going to be a physical piece on that. And so when you look at activities, and you're looking at this, and if you see an activity, you kind of want to consider these three things that we just spoke about, the means, the motive, and the opportunity. And you can try to determine whether or not that is a criminal activity, if it's an activist activity, what's happening.

Like I said, we all get spam in our email, how much of that spam is criminal? I would probably guess a good portion of it. How much of that spam is just unwanted email? What is the motive of that unwanted email? You know, trying to get you to switch your bank? Are they trying to get you to support Greenpeace?

There are so many different ways that people can do it. So we're all touched by cyber activity every day. And we need to understand what that cyber activity is, so we can build our response to it. And our response could be as simple as just hit delete on the email, but sometimes a response needs to be greater than that as well, because if your machine is compromised, or if your identity was stolen, there are things that you need to look at to determine what took place and how.

So when you describe it to a law enforcement, or your system administrator at your organization, you can give them an informed description of what took place, and what you think happened, and why, which could then lead them to have a more narrow focus on their search and their mediation, remediation to that.

Now, before I open up to questions, I want to jump around, and I don't have slides on this, I apologize. Why are we talking about cyber activities? Because we're ICANN, we talk about domain names, we talk about IP addresses, and you know, there is law enforcement, there is government entities, there is other places that handle and work with specifically criminal activities. So why is that important to ICANN?

The SSR team, Security, Stability, and Resiliency team, is a small team. We're only four and a half people, five and a half people. We do a lot of things, including training, exercises and stuff, but one of the things that we work on, more and more it seems, is that we work with law enforcement to help them understand the digital aspect of any case they might be working.

So when we talk about that cyber is not exclusive, or activities are not exclusive to cyber, that's kind of what we're looking at, and specifically in the unique identifier field. We're working on helping the public safety community, and law enforcements, and governments to help them understand not only WHOIS, which I think they got a good grasp on, but also the DNS in general, the system and how we can start using the DNS, and how the bad guys use DNS, but then how the law enforcement can use DNS to help build their case when they go before a judge to say, "We need to take these servers down because they're doing illegal activity, XYZ."

But now they have a trail, much like in real life, in their physical cases, they have to have a trail before they can ask for a warrant, or whatever it takes, some kind of legal action. We assist them in understanding what those trails are, what those fingerprint points are, on the Internet in order to help them build their cases and take action.

And then sometimes, in some cases, because the non-border aspect of what the Internet is, we also help coordinate activities. So if there is a command and control center for a large bot net, and we've determined that these bad domains are all being registered at one registrar, we will

work with the two organizations, the law enforcement and the registrar, to coordinate a takedown, because a lot of times, from a bad guy's perspective, if you see one of your domains seized, you're going to immediately change your activity, and change the way that you operate.

So we want to make sure that all of the pieces are in place, that all of the process has been followed, that the registrar can then, or the registry, depending on where we're going, can seize those domains all at the same time. We're not involved with any of the legal activity, we're just the coordinator between that, between these two entities.

We do a lot of that. We've been working a lot with law enforcement lately, mostly over the past year and a half or two years, it has really exploded, working with them on how they can determine, or how they can use the DNS to find abuse and misuse, and help their case, their cases.

So I'm going to stop there and open it up for questions, if anyone has anything.

ALAN GREENBERG: Alan speaking. Does anyone have any questions? And we have Alberto, who is presumably on the Spanish channel.

ALBERTO SOTO: This is Alberto speaking. I apologize for my voice, I have a cold. This is very interesting to hear all of this. In LACRALO, we have a training program, it's an internal program, that would also include cyber security

issues. And I am now going to include something related to what is cyber, by taking this presentation as a base, but I also understand that we would need to focus a little bit more, not only in whatever is raised to our individual users of the Internet, which is our aim, in the end, but actually we should also focus on the multistakeholder model.

Because in each event, in each webinar we have conducted, we have always had the presence of governments, and Internet service providers, the Civil Society, and the educational community, etc. But because, I mean, as LACRALO only, we would not be able to do this. So we would like to have some kind of participation and involvement so that we can do something together, so we can explain what ICANN is doing, and what we can do, so that we can reach to a greater audience in the multistakeholder model. Thank you.

ALAN GREENBERG: Thank you Alberto. Steve, do you want to take a few questions and then try to answer them all at once, or do you want them all one by one?

STEVE CONTE: However you normally do it, Alan, is fine with me.

ALAN GREENBERG: It depends on the speaker. Since we have Holly's hand up, let's go to Holly, and then we'll turn it over to you.

STEVE CONTE: Excellent, thank you.

HOLLY RAICHE: Okay?

ALAN GREENBERG: We can hear you.

HOLLY RAICHE: Okay, thank you. Holy Raiche for the record. Thanks Steve. Do you have a close relationship with both the GAC and to the different constituencies really that ccNSO? Because the picture you paint, particularly about the activities you have with law enforcement, getting governments to understand what you do and coordinate what they do with what you do, looks to be an excellent way to actually deal with, I hate to call it cyber crime, but cyber crime and/or cyber terrorism.

It just, it looks likes enormous potential for sort of cross ICANN activity. Thanks.

STEVE CONTE: Holly, thanks for that, and Alberto as well. I think, in some ways, I can address both questions with the same answer, and if I don't hit your question specifically, please ask for clarification. SSR team does work, we work closely with the global stakeholder engagement group,

because they have their foot on the ground, and they have the connections and relationships built with the governments and with other organizations in that region.

So we like to work within ICANN to coordinate with GSE, in order to reach out. However, your Holly question is spot on, and one of the things that SSR is looking to do is to increase our relationship with the various stakeholder organizations and advisory councils within ICANN. And, you know, this is one of the models, but we've spoken in front of the ccNSO, I think it was in London, we speak mostly on an one to one level with members of the ICANN community, but we're trying to reach out and make our relationship stronger.

And as part of this, and this was going to be at the end of the presentation, I haven't asked for your group because… So I sat in to some of the ALAC stuff, I believe it was either London or Los Angeles, I think it was Los Angeles. It was. And would like to see how we can coordinate activities and get the involvement of the At-Large advisory committee, more involved with the security and stability aspect of the ICANN model.

One of the things that we're doing is we're starting work towards a security awareness training, we're building it, unfortunately, we're building it slow because we are a very small team, and we're all out on the road quite often. But we're looking to do various things with basic security awareness, from the consumer level to a governmental level, of what you as a person, or what you as an organization can do to help the system in some ways, in order to make sure that that, you know, my son

is not clicking on emails that are clearly phishing emails and things like that.

So we're trying to raise the awareness so we can have bigger conversations, and smarter conversations, with entities. We're doing that with a training that we're building, and we'll be doing that with, probably a series of online learning activities. Right now we're developing an OLP model for learn dot ICANN that's going to be our foundation.

We're going to be doing an understanding DNS module that anyone can go in and, I'm sorry. Understanding DNS course, which anyone can go through these four or five different modules and get the foundation of what DNS is. At which point, then we can start building off of that. We're going to, once this is complete, we're going to solicit input from all groups, because we want to make sure, we're not building this for ourselves, we're building this for people like you on the call today.

And we want to make sure that we're hitting the right pieces, and we're hitting it at the right level, that the audience is getting valuable information from that. So another thing that we're doing is we're collecting a list of resources for security awareness. And I just put the link into the chat room. My ask to the ALAC, my immediate ask to the ALAC is to please take a look at that, and if you feel that there is a link or a site that we're missing off of that page, please do let us know.

We're happy to include it into that list. We give this list out to public safety. We give this list out to law enforcement. We give this list out to

anybody who we speak to, because we really want to drum up that security awareness and start from the bottom and work our way up.

Did that answer, touch the questions of Holly and Alberto?

HOLLY RAICHE: Speaking for myself, it's Holly Raiche again, yes it does. I'm just thinking of some of the activities that are going on in Australia. We've, for example, just appointed a person for children's Internet security, who used to head up the high tech crime this year, but it's the sort of thing where say, the Internet Society in Australia, could do a lot in terms of coordinating with the various bodies.

It's just a lot of information that probably should be disseminated and it would be really useful to have that link and see what's there, and work with that, as a way of using ALAC to disseminate a lot of the information, which I think would be really useful.

STEVE CONTE: I agree completely with that. Holly, please do take a look at that link, and if you're in Buenos Aries, I would be happy to have a conversation with how we can help the distribution model on that as well.

HOLLY RAICHE: Right. Thank you.

ALAN GREENBERG: Thank you Steve. Anyone else with anything right now? If not, I'll ask him a question. I guess it's my turn. I gave my first presentation on spam, I believe, in 2002. And I spent about six months ahead of time collecting every spam I got and analyzing it, and it was quite interesting. And I think I gave a first presentation on cyber crime, in a more general sense, probably about 15 years before that.

What do you see in terms of rates of change? Clearly, we have had ups and downs, and problems go from serious, to less serious, to more serious, but what are the overall trends?

STEVE CONTE: That's an interesting question. From my own layman perspective, meaning I am not privy to what law enforcement is looking at today, but what they communicate to us, a lot, some of the biggest changes over the past 10 years, I would say, obviously spam is just as bad as it was back then, but it's an order of magnitude because there is more people on the Internet and things like that.

We've seen more and more activities of phishing and people collecting data off of phishing, and law enforcement really is starting to, over the past three to four years, really starting to understand that they really need to get a grasp on these cyber activities, such as phishing. We just spoke to the FDA in London, I'm sorry, the United States, Food and Drug Administration, because they were very concerned about illegal pharmaceuticals on the Internet.

And that, when we talk about getting real, it's real, it's not just a loss of income for somebody, or identity theft, that puts lives in jeopardy. And so there are so many different new aspects coming in of cyber activities, criminal cyber activity, that law enforcement and public safety communities are really trying to get a grasp on what they need to do and how they need to do it.

But as far as [spam], I don't know if I can tell you, other than phishing, which sends to be like a big thing over the past year, I couldn't tell you specifically.

ALAN GREENBERG: Okay. Thank you. Could I ask people to please mute if you're not speaking. [Inaudible] background. And I'll ask again. Can people please hit mute? Thank you.

Alberto, and then we have Holly again.

ALBERTO SOTO: This is Alberto Soto for the record. Thank you very much. Steve, we are with our organizations, and in different countries, we are approaching Internet users, and we are talking about human trafficking, phishing, child pornography, and we are reaching, approaching those end users. In our last webinar, we had a presentation and the presentation had to do with the GAC and the Internet end users, and we spoke with the GAC chair, and we agreed on trying to participating in meetings to have a better relationship, particularly, because this would be useful for us.

Why? Because in Latin American countries, there are no laws regarding these issues, there are no laws governing these issues. And there are very few technical teams with a real capacity to cover these topics. And when I say capacity, I mean devices with equipment because equipment is very expensive. So, our task is also focused on trying to generate, in a bottom up way, the policy development, and the development of the different laws in the different countries, to cover and to approach these topics.

Because they may have the devices or equipment, the necessary equipment, but for example, they do not have the obligation to retain data. So this happens with Internet service providers. So if there is a crime, during the investigation of that crime, that are no data available. And that information is not available because it is not an obligation to retain that information, and to retain data.

So we have a very complex issue, and we are trying to face this whole situation. Thank you.

ALAN GREENBERG: Thank you Alberto. Steve, do you have any comments?

STEVE CONTE: Yeah, before we jump to Holly, that is an interesting comment, and thank you Alberto for that. I think if we were all sitting in the room, and I can do a litmus test on this in June when we're in Buenos Aries, and ask for a show of hands how many people from different regions have

that same struggle, I suspect we would probably see the majority of the room with their hands up. So, it's definitely an important consideration, but it's not a unique consideration.

And one of the things, you mentioned equipment and policy, and one of the things that I have seen over the past 15 years or so, is there has always been those two specific groups of policy makers and technology developers, and I think in the past, I would call it past five years, and some aspects to, you know, congratulations of Sally Wentworth and the Internet Society, there has been a lot of work, bringing these two groups back or together, to have dialogue.

And we're starting to see individuals who are involved with both policy and technology, and I think that will start helping, because policy can't, Internet policy, in my opinion, cannot be built without technology. And in today's day and age, technology really can't be built with having policy either.

It's no longer what it… The Internet is no longer what it used to be, and it has become, you know, I'm putting my fingers up, and putting it in quotes, it has become real. And so, these two separate bodies are becoming more and more integrated, and I think that's a very positive thing, and the more we can promote that, and the more we can encourage that, the better off every region will be in helping mitigate these activities, or these threats, and working with technologists and with policy development individuals, to create a better, more functional protocol, or application, or policies around that.

All of that, I think, will come together better.

ALAN GREENBERG: Thank you Steve. Holly?

HOLLY RAICHE: I'm going to ask a difficult question, you don't have to answer, but what challenges, certainly from your perspective rather than the ALAC perspective, have the new gTLDs, particularly the IDNs, posed for you guys?

STEVE CONTE: That's an interesting question. We've taken, when I say we, it's we as the SSR team, have taken a very close look at new gTLDs in particular, not so much as the IDNs, but just the new round of TLDs coming up. We're looking at it with a focus on where does criminal activity swing? So, you know, we do a lot of analytics and research to determine, you know, what registrar might be a, have more of a blind eye to their customers activities.

What registry might be getting more populated with criminal-esque domains. And so we've been looking at the new TLDs with that same model, to see, you know… As a new TLD comes up, what portion of the rush to that registration becomes based around criminal activity? I don't have any stats in front of me to give you, so I can't give you hard numbers, but that's what we do look at. And then we do work with the registrars and the registries, and provide them with the results, and say,

"This is what we're seeing. Can we help you in any way to help mitigate these activities?"

HOLLY RAICHE: Thank you. I think we'll have a chat about that in Buenos Aries.

STEVE CONTE: Absolutely.

ALAN GREENBERG: Anyone else? We still have a fair amount of time left, if anyone else has any thoughts.

Apparently, you've answered anything that anyone could possibly think of.

Any closing comments then?

STEVE CONTE: Only the strength of my message that, I really, when I was in Los Angeles at the ICANN meeting, sitting at the ALAC, I forget which function it was. I apologize for that. And sitting there, it really opened my eyes that I don't think SSR has spoken to ALAC enough. I've spoken to John Crain about this, it's my personal role, at the meetings, to have more SSR presence during ALAC meetings.

And I hope that it's not seen as infringing upon you guys' time. Please at any time, ask me to leave, but I find it very interesting what your advisory committee is talking about. And I think there are places where we can have very strong dialogue, and I'm hoping that we can strengthen the relationship, and build upon that.

And this is a great step. I appreciate and thank you all for giving us an opportunity to interface with you and create that dialogue.

ALAN GREENBERG: Thank you. A couple of comments. And apparently, there is another hand now, so you're not getting off that easy. And there was a question in the chat, it is scheduled as a 90 minute call, so we do have significant more time if people do have things to discuss. I don't think we're going to eject you from the room, if you show up at ALAC meetings.

An awful lot of what we do, focuses on, well, we're here to talk about the user. And implicitly, a lot of what we talk about is ways that, not necessarily the end user can be harmed, but ways that we can make the online experience for users either easier, or better, or safer. So implicitly, a lot of what we're talking about, do end up talking about SSR type things.

Not necessarily ones that are fully in ICANN's control, but certainly there is a large focus on that. So we welcome any participation. Olivier, I was expecting you to have a question.

OLIVIER CRÉPIN-LEBLOND: Thank you very much Alan. It's Olivier Crépin-Leblond speaking. Can you hear me?

ALAN GREENBERG: Yes.

OLIVIER CRÉPIN-LEBLOND: Well, okay, excellent. Thanks for this presentation Steve, it's very interesting. I'm always interested by cyber attacks, and cyber activism, and cyber "hacktivism," of course, because there is so much of it going on. And ICANN has recently been subjected to this through a spear phishing attack. And I wonder whether you can enlighten us as to what a spear phishing attack was in the ICANN context, and whether this was qualified as cyber "hacktivism," or anything else.

STEVE CONTE: Sure, thanks Olivier. So phishing is a more generalized attempt to gain a user's information. So if you get an email from somebody and it says, "Click here," and they're looking for your user and password, and you put it in, that you've been phished. They'll take that information, and chances are they're pretending that they're an entity that they're not, so they could be pretending to be a bank or something like that.

They'll take that information and they'll either use it, or they'll sell it, or they'll do a combination of both. In the case of spear phishing, that's a more targeted attack against an individual, in an organization, or a

group of individuals in an organization, in an attempt to compromise entry points into the network itself, or into the organization.

SSR isn't involved with the day to day IP security aspect of it, and I can't, and I won't, go into details on what took place. We were speak phished, I will acknowledge that. We had a general phishing attack, against the organization, and then we had a more detailed speared phishing aimed at certain individuals within the organization.

We, at least, as far as I know, we don't know necessarily who attempted to do this, and what their motives are. I know that the IP security within ICANN are still working within their own department, but also with law enforcement to determine, A) it was a compromise; B) what the motives were. You know, if we go back to that model of, you know, the motives and the opportunities, and all of that, we're still trying to build that picture up.

And sometimes, and often times, it's harder than it looks to determine who and why, because the Internet, you know, you can be the bald guy with the hairy arms and pretend you're a girl. It's the same thing with hacking and stuff too, is that you can put on a different face than what you really hard, and it's really hard to penetrate that façade sometimes. So it's typically, when it turn into a mediation so that you can immediately, once you have understood that you have been attacked, or phished, or compromised, from a physical perspective, you can take immediate action.

ICANN did that immediately. I would say within the first eight to 12 hours, there was action being taken. And so we can stop, or we, as ICANN, but we as an organization, not, it doesn't have to be ICANN. We took immediate action. We put other firewalls in place and other process in place, in order to help secure the network itself. And then the longer process on that is to, and Alberto mentioned it too, is to collect that data.

And hopefully that data is there to collect. We collect that data and we start building the story, and then start working with law enforcement to determine if there is a clear picture of who did it, how we can go about and take action against that.

ALAN GREENBERG: Thank you very much. It might be amusing to some people. My first experience what would now be called phishing, or perhaps spear phishing, occurred, I believe, on a 10 character per second teletype in 1968. The concept of being around for a while. Not nearly as onerous results, of course.

Any other questions? Dave, you have some things in the chat, is there anything you want to say? No?

Then Steve, you may have another opportunity for a wrap up, but you don't need to say the same thing over again. Last call for any questions, comments?

HOLLY RAICHE: Dev does have a question.

ALAN GREENBERG: Dev says, "Will there be a similar…" Oh. Dev is making reference to a number of sessions at previous ICANN meetings, and says, "Will there be a similar one in Argentina?" There is a session on cyber security, one on public safety, public safety workshop.

STEVE CONTE: So the public safety workshop is pretty much going to be an always things nowadays. That's where we get the public safety community and law enforcement together with members of the ICANN community, and start building and talking about things that are taking place. That's typically a half open session and half closed session.

I don't know what day offhand, I think it might be Thursday, but that's slipped a day or two, a day plus or minus, in the past. As far as specific cyber security, or SSR, events at Buenos Aries, I'm not sure yet. I'll work with John to, John Crain, to determine whether we have a slot, and if so, I'm happy to pass that on to the ALAC. Would that be via Terri?

ALAN GREENBERG: Probably. I would guess Gisella.

STEVE CONTE: Okay. If there is something going on with SSR specific, I'll make sure that Gisella has that information and can pass that on to the ALAC.

ALAN GREENBERG: Good, thank you. Last comments. Going, going, gone. Thank you very much for taking the time to do this Steve. I don't know, from my perspective, it has been most interesting and a little bit of fun. So I thank you.

STEVE CONTE: Thank you. And please, all of you, feel free to come up and say hi to me, I don't bite. I'll be in Buenos Aries the whole week.

ALAN GREENBERG: We'll try to remember that you don't bite. And by the way, thank you for contributing what be called, vaguely, as a poem at the beginning of the meetings.

STEVE CONTE: Limericks probably didn't qualify.

ALAN GREENBERG: Well, I don't know. It depends on how clean they are. But thank you again for joining us. Bye-bye.

[END OF TRANSCRIPTION]