LONDON – ICANN's Security, Stability, & Resiliency Team Outreach Session
Wednesday, June 25, 2014 – 15:30 to 16:30
ICANN – London, England

JOHN CRANE: Good afternoon, everybody. I'm just trying to round up my crew. I think they're all still in the bar – where we all wish we were. My name's John Crane. I'm ICANN's Chief SSR Officer, where SSR stands for Security, Stability and Resiliency. It's good having an acronym actually inside your title. We love acronyms here at ICANN. I want to talk today a little bit about what our group is doing, give everybody an update and introduce you to some of our team.

The technology works. It looks very 1990s, which is why it probably still works. Can people read that? That's not too bad.

Not all of the team are here and some of them are hiding in the bar. I'm John Crane, I lead this new group. It's a formation out of the old security group. With me, who's going to join us in a minute, is a gentleman called Dave Piscitello, who many of you may know. He's been in the industry for many years. He's VP of security and coordination.

We have a gentleman who's not with us, Carlos Alvarez. He's from Colombia. He was previously with our compliance team and moved over to us recently. He is very active in technical engagement and works a lot in the Caribbean and Latin American regions, the LAC regions, obviously Spanish-speaking. Despite my wife being Mexican I'm not very good at Spanish, which she berates me for often. He spends a lot of time down in Latin America.

Also not with us today is Tomofumi Okubo, formerly with the IANA department. He was instrumental in designing the root zone signing systems. He's moving over to work with us to a lot of analytical work and research.

Rick Lamb is our program manager for DNSSEC. He's around somewhere and hopefully will turn up.

Then we have Champika. He was with APNIC, which is the regional internet registry in the Asian Pacific region based out of Brisbane. He's attached to our Singapore office. He's doing technical engagement and outreach in the Pacific and Asian regions. He's actually out giving training right at this moment, which is why he couldn't be here.

Sitting at the table is Steve Conte. Stand up and wave, Steve, so they can throw things at you. Find out who you are.

As I said, hopefully Dave will be here in a minute. He was running over. We're all triple booked.

What do we do? Traditionally, the security group at ICANN did pretty much anything that sounded like it had security in it. We looked at web pages or websites we were developing, got asked to do last minute reviews of code, worried about physical security, worried about security at meetings. We were worried about what was happening out there in the identifier space. It was a pretty wide remit.

We formed this new group at the end of last year. Basically, our remit is to look at the identifier space, to understand what's going on out there, to be aware of threats and risks to that system, and to see if there are

things we can do around that system to improve the overall ecosystem. We split this into a few areas.

The first areas – I'm going to go into these in more depth – is around threat awareness and preparedness. Basically, if we see things out there that look like they're problematic – think about large-scale DGAs (Domain Generation Algorithms) – for botnets, etc. We get involved in things like that. Trust-Based Collaboration, that's basically working with the community, just a fancy name for it Some analytics or research and capability building.

Just walked in is Dave Piscitello, if you want to take off your tie and wave at the same time, that works. And Rick Lamb.

The first area we're going to talk about is identifier systems threat awareness. I'm pretty sure you're all bored of my voice already, so I'm going to make Dave talk to this. Being as he just ran – how far did you run, Dave? From the east wing.

DAVE PISCITELLO: I apologize for being late, but John and I were supposed to be in three different meetings. I was at one meeting thinking that that was the place where I should cover and apparently that was not.

As John introduced me, I'm John's vice president of security and ICT coordination. I'm going to walk you through the four, what John calls "pillars" or functional areas, for the SSR team. Then I'll introduce both Rick and Steve to talk a little bit about areas where they concentrate. You already talked about our new team and our growth pattern and the path to world dominance, right? Okay. Good.

What we call threat awareness and response is actually a very large part of our day jobs. We literally are active 24 by 7. There are lots of people in the public safety community who have our home numbers. We work with law enforcement. We work with security researchers. We work with people who are interveners in botnet and other malicious activity investigations to help them in situations where we might be able to provide some information or intelligence. We might be able to provide some connective tissue between one organization that ICANN may have a contact with, like a registry or registrar, and another organization that might be doing sink-holing of data or might be doing some sort of analysis of malware.

What we try to do is assist in monitoring DNS health identifying criminal use of the DNS, identify or coordinate takedown activities or actions. In some cases, law enforcement might come to us to ask how to better understand the identifier information they need to put in a court order. As an example, in those cases we try to help them by providing insight into the domain names, the registries, IP addresses and the like.

We also spend a great deal of time exchanging threat intelligence, things that we collect, things that others collect. We try to participate in responses and threats to attacks against the identifier systems. If we get advanced information about an imminent attempt to attack on the root, or attack a top-level domain in particular, we would try to put in motion some preparedness and some active countermeasures and the like.

The SSR analytics group, or function, is something that we are just beginning to develop. What we are trying to do is respond to a request from the community to provide better and more uniform root system

measurements and analyses. John takes the lead on that with the RSAC (the Root System Advisory Committee).

We're hoping that we will be able to come up with standards of the metrics and make those metrics available to the public for scrutiny, to researchers for deep dives into the data and analysis.

I focus primarily on registration abuse or misuse. We're coming up with some creative examinations of domain data, of domain registration data, of data that's collected through passive DNS. We're trying to understand patterns of behavior. We're trying to understand perhaps flocking behaviors of criminals; which registrars they're using, whether they're moving from one registrar to another. We work with actually some of the people in this room very frequently to try to say, "What are you seeing in your data? What are we seeing?" Maybe we borrow some data from people to compliment a study that we want. We work with some people to develop APRs into their data to try to explain what we need and to extract from the data they have.

In the future, hopefully by Los Angeles, we hope to have some reports that we will be able to publish. We're still staffing this function and it's still sort of a part-time job for three people who are 100% busy elsewhere.

In the future we're going to come up with hopefully some creative uses of DNS data. If you pay attention to the security space, you'll know that collecting DNS data and utilizing it for advertising, for surveillance, for intelligence has become one of the richest sources for understanding Internet behaviors. We'd like to understand how we can do that and use it in a positive fashion.

Trust-based Collaboration is where I think everyone on the team participates. It's a very intensive part of our function. We work – as I mentioned before, the Global Cybersecurity Cooperation is actually very much a part of our outreach. My ICT coordination hat on, this is where we engage with other stakeholders like the Message Anti-Abuse Working Group, the Anti-Phishing Working Group, the OECD.

Through our global stakeholder engagement we work with the commonwealth. We work with Caribbean stakeholders and we work with Asia Pacific to try to understand how we can share the knowledge that we have, our subject matter expertise, and to acquire some of that expertise and bring it in-house so that we can share it with the ICANN community.

The Global Security and Operations, there's obviously a little bit of an overlap here between the threat awareness and the security and operations. We work with many, many people in various vetted mailing lists to try to assist with research, assist with ongoing analysis, into botnet behavior, malware and the like.

One of the things that we're trying to do when we do all of these activities is take an eye to ICANN policy and see if there are things that we observe in policy that are having unintended consequences, that are giving criminals an opportunity to do something that perhaps they should not. Then we try to feed that information back into the community to see if there may be some need for policy reconsideration.

Under capability building, I'm going to hand this off actually to Steve. Steve has just come back on board to ICANN to all of our delight. He's helping us coordinate our training program. I'd like to let him talk about

some of the things that we're doing and give me an opportunity to catch my breath.

STEVE CONTE: Thanks, Dave. Can I have the clicker from 1977? Thank you all. We've been doing various tapes of capability training with the community since about 2003 in partnership with the Network Setup Resource Center (NSRC). We started doing training on targeting registries, mostly CCTLDs, and doing knowledge transfer and building skillsets with that group. We've since expanded.

In 2007 we expanded out. We did a contingency planning group with another partner of ours. Rick started doing DNSSEC training along with NSRC, but also with local exerts in region as well, which was really great because it was showing that DNSSEC was exploding and becoming more popular, but also that those who are at the courses also have an opportunity to know that there's a regional expert. I'm actually going to pause here and pass it onto Rick. Get a little bit more in depth about your work with DNSSEC and other training. I'll take over again from there.

RICK LAMB: Which button's for explode? As Steve said, I benefit very much from the ground work a lot of these guys had already done. Luckily I came in and finally started to be able to do some of this training. Looking back a little on the Trust-Based Collaboration, one of the things I've learned – and these gentlemen have known for a long time – is that in doing these trainings, we're really building people networks.

The law enforcement training, the DNSSEC stuff that I do, in the end what I realized is that everyone in the room now has been forced to be somewhat secondary, or something like that if it's a DNS class, if you guys know what that is, or something better.

I've had people from law enforcement come to me in some of these classes to say that, "On a Saturday night I have some sort of problem going on. What's the chances of me contacting my counterpart and getting them to react and help me out in this?" It's that human networking that he has said makes this work. Not some sort of top down structure or something like that.

That being said, we've really been fortunate. Some of the places we get invited – OAS, for example – they'll bring us in to talk to ministers trying to create a national cybersecurity frame work for their countries. Because ICANN is such an expert in the multi-stakeholder model, many of them have embraced that and realized this is something we need and they're trying to build on our knowledge.

Then in the DNSSEC stuff, of course, that's hands-on training that we do around the world that's free. Again, part of is the technology. Most of it is the networking that we get out of that and the goodwill, to be honest, for doing those things that are usually week long things in strange places. That's pretty much what I focus on. Steve is going to try to coordinate all of this and make all this stuff much more effective, I think, than it has been. I do appreciate that.

UNIDENTIFIED MALE: Before you relinquish the mic, about how many countries have you touched with your DNSSEC training?

RICK LAMB: You're putting me on the spot here. You really are. I haven't been doing it that long, but I think probably about 15 at least, personally, that I've had to go with NSRC and sometimes with the people on the ground, as you pointed out, which was really helpful.

STEVE CONTE: Thanks, Rick. We started the DNSSEC training, we expanded our market from there and then we started looking elsewhere. In about 2012 Dave started looking at the public safety community and really started looking at what we could do to law enforcement and other agencies that could benefit from our remit of looking at stability and security and resiliency of the unique identifier systems on the Internet.

We, of course, do boot camps and whatnot for staff, bringing new staff on board. If you're not in the community, I'm sure you have all gone through the nightmare of acronyms. I'm trying to understand what the DNS is and all that as well. We work on that.

We are looking, coming soon to an engagement near you. We started exploring a new track that we're currently calling security awareness. It is not developed yet, we're just in the infancy stage on that. I suspect you'll probably be seeing that in the beginning of 2015 and we'll start being able to promote that through our global stakeholder engagement team and the regional vice presidents there within.

Our audience, I've kind of already brushed on this so I'm not going to spend too much time, we started with the ccTLD registry operators and it's still pretty much a key focus of ours. Through some of our courses, though, we've noticed that some of the registrars have also come to join our engagements and our events.

We're looking at the contingency planning. Although it was developed in 2007 we're doing a revision of it now and hopefully having it more broadly relevant to communities outside the ccTLD registry. We're continually evolving our courses. We're looking on how we can be more impactful within our community as well.

Dave talked about the operational security and public safety community. Obviously the technical community, the work that Rick does with DNSSEC, and we also have various other network security meetings. In fact, I think Champika is in Singapore right now at a SGNOG doing technical trainings. When it's relevant to the SSR, then we're happy to be there.

Other audiences, as defined by our regional vice presidents from around the globe, the GSC determines and looks at if there's a training that we could provide that's relevant to their group and their communities.

I'm just curious, out of the room, how many here are CCTLDs, if any? A handful. How about registrars? Okay. How about regular gTLDs, new and/or existing. Okay. Excellent. And how many "other"? All right.

There's a great source, if you're interested in training, please reach out to your regional vice president from our GSE team. We would be happy to sit down with you. Or find me after the session. Happy to sit down

with you if you guys are interested in training, if you have an event that's coming up that has something that is relevant to the unique identifier system, security, stability, resiliency group within ICANN. We would love to talk with you, would love to get on the ground and spread our knowledge. That's what we all love doing.

UNIDENTIFIED MALE: Feel free to contact us directly, too.

STEVE CONTE: Absolutely. We are trying to be more holistic and strategic in our offerings. Typically, in the past – and it's just the way things are. We've always been very reactionary and trying to facilitate an event sooner than we actually want to because we don't have all the pieces in place for planning.

One of my remit is to come in and look at this from a more strategic point. If you have an event, even if it's the middle of next year and you think that something's coming on, come talk to us. We'll mark it down and we'll start working on it. We'll see if we can facilitate that. That's my ask to you guys.

Actually, I have two asks. Also, what are we missing? So many of you have been in the community for quite some time. As I mentioned, the courses we have, we understand that we've been doing the registry operations courses for a number of years now. It's solid and it works, but what else could we be doing that fits within our remit? What else could we be doing that benefits the community and brings a more stable and secure Internet out there?

I am personally extremely interested in that. If you have an idea of what could be taught that's not being taught, I encourage you to find me here at the meeting. My e-mail is up on the slide deck (steve.conte@ICANN.org). I would love to hear and listen to you and hear what we could do to improve our training courses.

I think, John, with that, I'm going to pass it back to you.

JOHN CRANE: Rather than us just talking at you, we thought we'd do a short overview then patch straight over to questions. If anybody wants to ask us questions about anything, feel free. We may tell you it's nothing we know anything about, but feel free to ask. If you could step up to the microphone, please.

STEVE CONTE: I'm sorry. We have people online, so if you could speak your name and affiliation, if any, as well, please.

CASS GOLDING: Sure, Cass Golding from Nominet UK TLD. What you guys are doing in the global initiative is absolutely fantastic and very much appreciated. As you pointed out, you're under-resourced, doing three roles at a time – have you thought about doing train the trainer sessions, where you can put it out to countries so that we can work in that community?

STEVE CONTE: That's a great question and I'm sorry I didn't bring that up. We actually are doing train the trainer sessions on a more ad hoc. In fact, Rick you're going down to Africa with [inaudible] IANA soon to do a train the trainer.

Again, looking on a more strategic level, and especially around scalability, where there's six of us on the team, train the trainer is very important to us. We want to bring that more to the forefront of our remit and try to get more people on the ground and ready for that.

JOHN CRANE: The other side is that we're very interested in looking at online interactive training mechanisms so that we don't have to sit for hours in airplanes to train people.

[JOHN CRANE]: With that being said, I'm going to be the bug in this soup. I can do that too. There's nothing like being there with each one of the students. Some of it you have to be there to convey certain things and to form certain relationships. Train the trainer is definitely a direction we're going for, but to transfer the motivation, the desire to do this stuff, you actually have to sometimes go to these places. We're never going to completely get rid of that, but we're going to try to make the most use of the small team that we have.

STEVE CONTE: We also have two staff who are going to actually take a yeoman's role in regional training. Carlos Alvarez is probably awaiting the arrival of his

second child, so he's not here. His wife is delivering today. We're so busy that we're actual scheduling deliveries. But Carlos is actually preparing some of our training in Spanish. He will be taking over the South American region. He already, the day before he took his paternity leave, he gave a two hour training on DNS basics in Spanish, with Spanish material.

Next month I'm going down to Singapore, Auckland, Manawatu and Brisbane to train one of our other staff. Champika speaks Chinese. Hopefully he will actually eventually migrate some of that material so that we can deliver it in that language.

We just had this week a request from Interpol to work with them and do train the trainer programs for their MiddleEeast and Interpol staff in French. We're hoping that we'll actually be able to train their staff to deliver our material to the Interpol agents in French.

We had a nice meeting a couple of hours ago with a woman from an organization called Together Against Cybercrime. They're based in Strasbourg University. They are very interested in the possibility of helping us deliver in French, and the woman that I spoke with actually said that they might be able to do it in Russian. We're very close to possibly being able to offer some of our courses in all the UN languages, which I think is pretty cool.

Yes, we're really interested in actually getting anyone who would like to train. The material, we developed, so we have it. We're happy to share it and to work with you to figure out how to deliver it.

CASS GOLDING: Thank you for that. I do have another question. This is about DDoS attacks. You talked about gaining threat data and botnet activity. Obviously botnets are often used for DDoS attacks. Are you collecting data regarding DDoS attacks using DNS?

JOHN CRANE: We ourselves are not. There are people out there collecting this data that we know. It's a lot of data to collect. We're watching it. We've had a couple of cases that through our threat intelligence mechanisms, we've become aware of threats against specific name server operators and we've passed on that intelligence. We had a very specific one against the root servers at one point that made us circle the wagons.

If you look at some of the DDoS data out there, it's staggering and very scary. I'm not sure that all the UDP attacks are going to be DNS anymore. They're moving onto other stuff like NTP, etc. So we're very aware of what's going on from a sort of threat intelligence standpoint and following it, but our analytics and data stuff is something that we never had before.

To be frank, I think if we'd said this a year ago, that we were thinking about doing this, there would have been a lot of people in the community who said, "You shouldn't." But if we don't have our eyes on the data, we're going to miss this stuff.

We work for the community, so we get these things and we pass it back to the community through secure mechanisms if we know somebody's threatened. We hope they'd do the same to us. This is very much a collaborative effort. I wish we had that kind of data.

[END OF TRANSCRIPTION]