TORONTO – Experts Panel on ICANN Security (DNS Abuse Forum)
Monday, October 15, 2012 – 13:30 to 14:45
ICANN - Toronto, Canada

BRAD WHITE: We have empty chairs up here. We're just solving a couple of last minute problems on our remote participation then we'll get under way.

Okay folks. I think we're going to get started. We want to make this session a little bit different than many of the other sessions you may have attended at ICANN. We want this to be as loose as possible. We want this to be as interactive as possible. We want to entertain as many questions.

In other words very unstructured, very participatory. That's what we're after here. We've got a great panel talking about security. This panel is virtually unmatched. Let me introduce them. Start at the end.

Jeff Brueggeman is Vice President of Public Policy for AT&T. in his role he's responsible for developing and coordinating AT&T's Public Policy positions on the Internet, technology, and broadband issues.

He leads the development and coordination of AT&T's strategic policy initiatives related to advanced technologies and emerging services such as broadband, security, Cloud computing, and converged IP services.

The gentleman next to him I have no idea who he is so we'll skip him, Dr. Steven Crocker the ICANN's Board of Directors. He's also the co-founder of Shakuro Corporation dedicated to the employment of improved security protocols on the Internet, primarily DNSSEC.

Steve is an Internet pioneer who helped to establish the protocols for the ARPANET, which of course became the foundation for today's Internet.

Next to him is Jeff Moss. He's our Vice President and Chief Security Officer. Jeff is better known as Dark Tangent, somewhat famous or perhaps infamous, hacker. In 92 Jeff founded DEF CON, the largest hacker community and gathering in the world.

Then five years later he started Black Hat, a series of technical conferences featuring the latest security research. In 09 Jeff was appointed to the DHS, Department of Homeland Security in the US, their advisory council which provided advice to the department. Is that basically right, Jeff? It's a long bio; I had to really boil it down for you.

Next to Jeff, Debbie Monohan is the Domain Name Commissioner for .nz, the New Zealand ccTLD. As such she's responsible for the oversight of the NZ domain name space. She also is responsible for setting the policies, authorizing registrars, monitoring the performance of the registry, NZRS, against the service level agreements.

The famous Dan Kaminsky, he's a noted Security Researcher. That's kind of an understatement. For over a decade he has spent his career advising fortune 500 companies such as CISCO and Microsoft.

His claim to fame is finding a critical flaw in the Internet's DNS called appropriately the Kaminsky Bug. We really want to thank you for that, Dan. He led to what became the largest synchronized fix to the Internet's infrastructure of all time.

Next to him, never mind we don't care about who is next. No, Dr. Paul Twomey, another former ICANN CEO. He's the Managing Director of Argo Pacific, high level International Advisory firm which assists companies to build and grow Internet and technology businesses.

He was our CEO from 03 to 09. He's a former chair of the World Economic Forms Global Agenda Council on The Future of the Internet. So like I said, a pretty distinguished panel.

Again, we want to really keep this as loose as we possibly can. I'm going to ask the first couple of questions. But when you guys are ready, go to these microphones and we do have a remote participation person here, Margie.

She's going to let me know when we've got questions from people joining us online. I just want to throw up the first question to you, Steve, just for the sake of clarity. What exactly is ICANN's role when it comes to security?

STEVE CROCKER: I appreciate the short easy questions. I'm pausing because I'm editing out all of the temptation to say, "It is not xyz." ICANN's role in security stems from its mission to coordinate and oversee the unique identifiers which is sort of bland code word that includes, but isn't limited to the domain name system, top level portion of the domain name system.

But it includes the addresses and autonomous system numbers that go with that. And the publishing of the ITF protocol parameters. Then in our involvement in the marketplace with the gTLDs, the registries, and the registrars in trying to oversee a little bit of sanity and clean

operation of those, security is a big word. It encompasses a lot of different things.

People read various things into it and Internet security is, in my experience, not a precise enough term. Because it includes everything from phishing to attempts at extortion to espionage and a variety of other ills, some people view spam as an intrusion. That is a security violation. Other people view harmful content because it stirs the emotions of the populous as a security issue.

Our mission is really very narrow in there. We care an awful lot about the stability of the Root Server Operations. And we care even greater amount because we have a very direct role in the quality and accuracy of the information that's in the Root Zone. That's a very specific and very narrow area.

We care a lot about the operation of the domain name system generally which is why we're very supportive of DNSSEC. On the consumer side, if you will, we care a lot about the operations of the registries and the registrars so that there're limited amounts of fraud and abuse from that area. Jeff Moss can say quite a bit more about all of that.

BRAD WHITE: Which kind of leads me into the next question, Jeff, you were talking before this session began. You were mentioning to me that you can see a possible disconnect between what ICANN's mission is in the role of DNS Security and what our perceived mission is. Can you talk a little bit about that?

JEFF MOSS: I'm mostly interested in, since everything ICANN does, we're very community supported and we do have a limited role in Remit, as pointed out by the SSR It just recently asked ICANN to publish what we believe a short and concise view of what is ICANN's role in Remit and Security at SSR.

That comment was out to the public and it's in draft form right now and so we're getting ready to publish all the community feedback. But it's really interesting the difference between what ICANN internally thinks its role is the difference between what the community and different members of the community have different views.

So when you say that ICANN is the coordinator for the global DNS system. It really hinges on what the word coordinator means and if you're a country that has no Root Servers in it and there's some interruption in your service you might think ICANN. I'll go to ICANN and talk to them about it.

They're the global coordinators, the buck stops with them. If you talk to Root Operators, the buck doesn't stop with ICANN, it stops with the Root Operators. So there's sort of this disconnect and the more that's clarified the better.

It is not just for ICANN but the better it is for the community to understand what the expectations are. I think with improved or increased attention from governments, the more we can clarify this and the better we're going to be. The more ambiguous this is, the more confusing it will be, not just for the GAC but for everybody.

BRAD WHITE: And in our discussion, when you and I were talking before this session began and we were talking about the anonymous threat, which was we established February I believe, February of this year?

You brought up a really interesting point I thought and that was you were saying there were a lot of people when that threat was being publicized and they're going, "Okay, we have to get somebody on the phone. We need to call the Internet."

JEFF MOSS: Yeah, there was one government that was like, picks up the phone, "Get me the Internet!" that's not going to work. And so you start researching, who is the Internet. And to them, ICANN was the Internet.

We have this thing that's published that says we're the global coordinators. And so that must be who you call. And I was talking to one of the Root Operators.

I said, "Yeah, isn't that an interesting situation to be in?" and he said, "Yes, yes I don't envy you at all because you have it written down that you're the coordinators.

I don't have it written down that I'm the coordinator. So all I have to do is best effort. I'll try really, really hard to keep my service up. But if I fail, I tried my best. If you fail, it's written down on your piece of paper, not on mine, interesting situation to be in.

BRAD WHITE: Paul, since you were CEO, have you seen security concerns as regards ICANN change. Or perhaps better stated have you seen expectations change?

PAUL TWOMEY: Well, a couple observations, first starting off where Jeff just left off. I think you'll find that in the period that ICANN's been in existence the interaction with the Root Server Operators has been one I think of attempted engagement in corporation.

I think the Root Server Operators, if they'd actually understood what the intent was at least of the US Government in 1999-2000 was much more diversionary than actually occurred. And so they have been doing obviously a good role in the coordination realm.

But I applaud this new charter for the OSAC and for the Root Server Operators coming closer into the ICANN process for a couple of reasons. For the reasons that Jeff just pointed out, the reality is about that part of the infrastructure that there needs to be an umbrella.

There needs to be a space in which more stakeholders are involved if necessary, if crisis were to occur. And I think all stakeholders involved in thinking through what resilience means in that space.

So the question that was put out for public comment about, "Shouldn't ICANN look for processes of transitioning the Root Server?" I think the answer to that is absolutely. And the Root Server Operators obviously should be involved and they should just get on and do this because I think time runs out.

JEFF MOSS: I'd rather have it happen under our time control than have it compounded onto us due to an emergency.

BRAD WHITE: You seem to be talking about that like it is inevitability rather than, I mean you both seem to have this sense of it's got to happen.

JEFF MOSS: So I think it's only happened twice in the past. It sort of just happened. There wasn't really a procedure. I think one was through the acquisition of another company. So in the future you could imagine another acquisition of a company.

You could imagine a situation where a Root Operator just decides I've done this for a long time, I'm retiring. Well then does he hand it off to his buddy or does it come back to ICANN, does it go on eBay? I mean, who knows? So it would be really nice to have some clarity and predictability there.

BRAD WHITE: Debbie, how do you see from your position? How do you see ICANN's security role?

DEBBIE MONOHAN: Well, as a ccTLD ICANN doesn't have an operational role in our security aspects of ccTLD. So I suppose in that respect what we would seek is, I agree there needs to be some coordination across. And ICANN is in a

good position to bring across multi stakeholders' views and come up with some good guiding principles, some guidelines, and some documents which a ccTLD can look at.

And either choose to implement some, all, or none. Because ultimately, they will run the ccTLD in a way that suits their country. Just picking up on the discussion about Root Server contracts, we've signed an Exchange of Leaders with ICANN and that actually included ICANN securing instability of the DNS.

Now the question is actually how can they sign up to that when there's no documents that they can point me to show on what basis they're actually being run by.

I think that to me one of the roles for ICANN is to look where the gaps actually are and to have document and processes in place which is pretty much how a ccTLD actually runs.

And ccTLDs can actually share some of our stuff because we're all parading in the same space in quite often a more nimble and quick way. And we're one of the key stakeholders that ICANN actually has. So to me it's they don't have an operational role in running .nz or the security aspects of .nz.

But having said that, I think when I only use the database to alert about Conficker, we then as a registry put our own solutions in place that suit us for that particular set of circumstances.

So I think raising the flag and raising awareness, great. Leave it then to the registry to figure out how they want to run it themselves.

BRAD WHITE: Dan, I want to hear from your perspective. What is the greatest threat that you see right now to the DNS?

DAN KAMINSKY: There're an awful lot of people who want to mess with DNS lately. They're not just hackers. I'm pretty concerned with the rise of Denial of Service attacks against DNS infrastructure. We've been defeating them for a decade by just throwing bandwidth at the problem.

And the other side is now throwing bandwidth at the problem too. And it's turned into a substantial arms race. It's turned into a matter of scale. Between the Denial of Service attacks that I've seen growing at exponential rates and the actual compromise of registrars and registries, what I am starting to see is a lot of force being applied on a scale that is larger than we're all comfortable with.

What I mean by that is there's a lot of desire for independence in the DNS space. We've got our rice bowls. We've got our little areas, this is what we do. Other people can maybe advise if they feel like, but this is our space.

That works up to the point that you have surprisingly powerful actors exerting force at which point you need surprisingly powerful push back. That is actually a role I like seeing ICANN take.

There are needs for coordination. There are needs for organization. The response to Anonymous, I was telling Jeff earlier, threatening the DNS may be the most valuable thing Anonymous ever did. It's like a vaccine.

There's no actual threat but my goodness did it create an immune response.

The DNS got a huge amount more stable because of a synchronized threat where there was no actual threat. I'm hopeful. I do see that there are significant threats out there. But I do see that there is a willingness to respond to those threats as a coordinated group. So that's kind of my opinion on the situation right now.

BRAD WHITE: Let's deal with that issue of coordination. Shortly after I started working for ICANN they dealt with Conficker, the Conficker threat. For me, as an AFI coming into this world, it was amazing to see all of the various segments kind of joined together to fight that threat. Is that the model for a future sort of defense against that type of threat?

DAN KAMINSKY: I think there's no other model. We're stuck together. The scale of threats that we're seeing now are on an order of magnitude more than what we would have originally liked them to have been. We have to work together to fix some of these large things.

Like Conficker and the attacks that are coming, no individual registry, no individual registrar, no individual organization can deal with them alone. We are actually going to have to coordinate and honestly the time to set up that coordination is before the attacks actually start.

JEFF MOSS: The benefit of the Anonymous threat was actually all the coordination work that happened. So what will you do when the attack happens? Those preparations can be used for any future threat. I want to echo what Dan's saying.

The thing that's been keeping me up at night is the size of these DDOS flows. They're getting kind of crazy. At the time of the Anonymous threat, we were looking like what's the biggest flow that anybody has seen. Then that will be sort of near our upper threshold.

It was 132 gigabytes back then. So that's a pretty big flow. So the attacks against Wall Street last week, 212 gigabytes, you went from 132 to 212 in less than a year.

I don't like that chart and I don't know how you defend against that unless you just have lots and lots and lots of any casts and lots of bandwidth to localize the effects of these flows.

Because if they can aggregate you're in trouble, the way that some TLD operators work, all their servers are in one country, sometimes in one locality. By the time all that traffic aggregates in your locality or in your country, it's all over.

You've got to limit this stuff. In my view you've got to limit it as far away from home as possible. I would like to see more coordination around a unified strategy for limiting 200-300 gig flows.

BRAD WHITE: Sir.

ERNIE DANIELS: My name's Ernie Daniels from Afilias. We're certainly concerned about the increasing Denial of Service attacks. But there's some additional factors coming into play now that maybe weren't known or weren't being used in the past.

In the early days, Denial of Service was off due to a fault that was discovered. Like some of the early ones with the syntax. So the solution for that was to patch your TCP stack and get the software right there upgraded.

That strategy has become a lot more difficult with the Botnet because it's extremely difficult to identify all the client machines, and get them patched. But dealing with that we've known about that issue for some time.

I think there's another factor that I'm not aware of that how much has been addressed which is beyond a fault in the system that you can repair. It has to do with the design of the protocol whereby using the protocol in the way it was meant to be. You can actually get a reflection of a huge magnitude beyond the input.

I know that DNSSEC particular is prone to this. I'm not sure what other protocols might have this underlying fault that either is known or hasn't been discovered yet.

I'm just wondering what's going on in the industry on the part of looking at strategies for Denial of Service that is dealing with not patching things but dealing with design faults in protocols.

DAN KAMINSKY: So DNSSEC is not particularly special in its amplification. There have been some claims but what you actually see in the field is that when amplification happens, it doesn't even bother with DNSSEC.

They just use straight DNS and it is fine. At the end of the day, our fix for most Denial of Service has just been let's just having more bandwidth than the other guys do. We've got money, clearly maybe they don't.

We'll just brute force our way out of this problem. At the point where we're getting 212 gigabyte flows, brute forcing our way out of this problem is not scaling anymore.

That's kind of the theme that I see honestly for the next decade. We have a lot of solutions we're comfortable with, not all of them work once we're four, five, six orders of magnitude more than we were originally designing for.

So do we see protocols getting redesigned? Do we see networks getting redesigned? If we do, that happens on the technical layer but it also happens on the policy layer. People have to agree yeah; maybe we should look at interesting things like how do we deal with spoofing, with spoof traffic?

What do we do about requiring protocols to validate that they're communicating with a peer? How relevant is it that they are communicating with a peer when you're in a Botnet and the attacker actually does control a few million machines?

One of the most interesting things about Conficker, by the way, is to this day we still don't know what they were trying to do. We know they

broke into a bunch of stuff. We know they held onto that stuff as hard as they could. But what they were doing, we still don't know.

BRAD WHITE: Steve, you wanted to add something?

STEVE CROCKER: Thanks Brad. So I agree with everything that Dan said. Dan, you mentioned a couple of things. Reflection, and it doesn't depend upon DNSSEC, it can use DNS alone. Underneath all of this is the mechanism that's being exploited with these reflection attacks is a false source address.

So a package gets sent in to a DNS resolver with a fictitious return address. In fact the return address is the target of who you're trying to attack as opposed to who the sender is. The agreed upon mitigation of this and reduction of this is to check the source addresses upon entries.

So that ISP should not be letting some user or some machine send in a packet that is clearly mis-advertising where it's from. It goes under a number of rubrics. There's an RFC that describes it, a Best Common Practice Document Number 38 and there's gathering attention.

Not as much as we'd like, but gathering attention on trying to implement this across the ISPs, and I think one of the things that will bubble up for attention is an assessment of where we are on that process and how effective it is or it isn't.

BRAD WHITE: Jeff.

JEFF MOSS: I certainly don't have anything to add on the technical issues but I did want to point out that I think these attacks are also creating political concerns that we all need to be aware of.

That is, the worst case scenario, an increasing desire by government to have one place to go to call up the Internet to get these problems fixed. Having been on the Security Review Team, while we were conscious of making sure that ICANN didn't overstate its role, we also are concerned.

And were concerned that governments in particular as cyber security becomes a bigger issue on their radar screen are not understanding what is happening today and potentially looking for more of a government role in being the solution to this.

We see this in terms of public/private partnerships and other issues. So I do think while we are wrestling with all of the technical issues, to some extent it's an opportunity to show that the lack of centralized control is not a flaw. It's actually a benefit to the way the Internet is designed.

ICANN I do think plays a critical role in being a helpful not just a formal coordinator but a really important body that brings together technical expertise and all of the operators of the infrastructure in a way that be very helpful.

PAUL TWOMEY: Can I just add to that clarion call? There's an old phrase about read the signs of the times. One of the things that I even got worried about more this week is the US Secretary of Defense's statements.

Two days ago or three days ago about a pretty clear warnings against third countries about having infected critical infrastructure, statements about their type of warfare doctrine about to be released.

I think it's pretty urgent, frankly, for the ICANN community generally, the broadly defined, to really work through clearly the multi stakeholder approach around things like the Root Servers.

How they're operated, the Root Servers and how they're going to be, you know, any potential change issues around DNS, issues around compliance, around registrar behavior, etc.

And be clear about the roles around that because I am concerned that we will find ourselves in some situation where an offline conflict is going to produce an online conflict.

Governments traditionally have had a concern about the Internet where most of the concern has been really around content. But in the rise of cyber espionage and then potentially in cyber conflict, it is absolutely about the networks and the infrastructure.

And my concern is if the ICANN model and community is around multi stakeholder and transparency, then there needs to be a lot of attention, I think, paid around this issue to pre-empt if there's a crisis happens. Because if it's not clear when the crisis happens, all hell will break loose.

BRAD WHITE: I'm just curious in the scenario you just raised, you said that the terrestrial, conventional sort of conflict might rise followed by the online conflict. Why do you phrase it like that? Why couldn't it?

DEBBIE MONOHAN: And I think it's very important to understand that and to make it very clear. When I hear about that there are countries which have their name servers all in one country. I know countries that have only one uplink to the world.

And I can tell you if this uplink is down, this country is down, is disconnected. I think it's very important to understand and distinguish what's DNS related and what is not DNS related which relies actually in the infrastructure itself. The infrastructure, it relies on the, let's say the cabling.

So when we talk about the cabling, it's like a street network. You can't guarantee that each street in Africa is as prosper, is as easy to drive, as a motorway in the US, of course not. It will not. Of course there will be cases where you actually can't reach that village in Africa through the Internet.

So we should really understand what is DNS? What is not DNS? What is TCPI? What is TCPI related? When we talk about the protocol, it's a packet switch protocol. When we talk about DDOS attacks, nobody actually would argue that if you say in the mobile world.

If on Christmas evening everybody phones his parents and only let's say ten percent actually get connected that it's a DDOS attack, of course

not. But 90% couldn't get connected because it was within the protocol that it's a point to point connection.

So the protocol guarantees a point to point connection. We now have within the Internet a packet switching network that is underlying in the protocol. If there is a packet switch that if too much people put too much packet on the network that it doesn't work anymore.

We have to make the people understand that. We shouldn't tell them and explain to them that we can solve the problems, each and every problem.

We have to address that we have to distinguish. That I think is very important to be transparent in what is possible, what is not possible, and what is DNS related and what is not DNS related. That's my comment.

DAN KAMINSKY: So I was in this amazing meeting. I was talking to 200 engineers. I'm like, "All right, guys. How many of you write software that depends on DNS?" and two hands go up out of 200.

I'm like let me rephrase my question. "How many of you guys have software that expects that it can take a string of text and get back an IP address so that you can make a network connection?" and then 198 hands go up.

Everything is a DNS problem. It's this really interesting foundation in which we build these protocols that expect that they can communicate across organizational boundaries. And the only reason that these

protocols are able to do this is because the DNS gives them that capability.

What we are in fact seeing is that a surprising number of actors, hackers but not just hackers, are realizing if they manipulate the DNS, they can manipulate all of the larger protocols. This can be for reasons of cyber war, this can be reasons of activism, and this can be reasons of some teenager having fun and fraud.

There's a pile of reasons to mess with the Internet and it turns out that DNS is this really nice point to poke at. Just because, imagine an entire country's uplink goes down. That doesn't mean that every single site in that country is down. Sites in that country might be hosted out of the country, might be hosted globally via a grand Anycast system.

But you attack the one DNS layer and none of it matters because no one can find those addresses. So we have this interesting inflexion point, or targeting point, for a lot of attackers where it's like, "Hey, however else things are going on there, if you hit here, you get to break everything built on top."

You see a lot of people that have various interests in changing the Net. There're these four standards, security, sovereignty, privacy, and piracy, various forces that are trying to change stuff.

But there's one force that is really the one thing that I think binds every single person in this room which is reliability. We've built something amazing here; it's got to keep working. It is remarkable how many people not in this room aren't considering the reliability story.

BRAD WHITE: Sir.

RICK WESTON: My name's Rick Weston. Thank you all for taking the time and taking the arrows for security. I think that the conversation that I've had many times in the cyber security realm has been tracking more towards cyber warfare and the duality of this online capability for a kinetic effect and vice versa. That's very scary to a lot of people.

I think that ICANN is in a unique position to help coordinate many of the aspects of the Internet and keeping it stable, reliable, keeping it up.

I've found that if we could pivot the conversation from security into health, we would find that there's so much more latitude for a healthy Internet, for bringing systems into a healthy place.

We see it in our nation with weight. There's many more friendly ways of having a discussion about how the Internet works in a positive way that benefits the global community, regardless of your national or sovereign status.

So what I would like to see ICANN do is create an effort that pushes cyber health or the health of the Internet or like the WHO. The WHO does an enormous amount of collaborations within the health community because they have the relationships.

That's what ICANN has. I think that's where its value is to the global community and to remove ourselves from the conversation of war I think is a healthy thing for populations in general. Thank you.

BRAD WHITE: Sir.

SIMON MCCALLA: Thank you. My name is Simon McCalla from Nominet UK. This question is for the panel. We talk back on DDOS. We tend to I think us DNS experts tend to focus on sort of the monolithic approach, we must fix the DDOS problem by as you say bandwidth and whatever else.

We've been working with the ISPs in the UK to look at how do we reach out to the customer and try to fix the DDOS problem that the customer is in. but the problem we have in that debate is that a perceived lack of, like a trade-off of privacy.

You start helping the customer understand what traffic there sending by the very nature you're starting to monitor and look. So the question, I guess Jeff probably it's a good one for you actually as an ISP. How do we tackle that issue of helping customers to improve their own DNS health without feeling like we're invading their entire privacy?

JEFF MOSS: Yeah that's become a big issue generally not only for the consumer facing issue but also the information sharing and finding ways to improve the sharing between private sector companies and with the government.

I think what we've tried to do is address that with structural protections to make clear that if we're going to have to get into an individual issue with your computer or your service, then obviously it's a very heightened privacy concern.

A lot of what, my understanding from our security team, a lot of what we're talking about is signature threat information, traffic flow data, and other things that can be shared in a way that does not raise that personal privacy type of concern.

I also think the issue of what may be a trade-off in terms of how do we address these threats in a way that preserves the open Internet is going to be a big issue as well. Again, the best answer in my mind is to have a transparent solution so that there aren't any surprises in terms of what ISPs are doing.

BRAD WHITE: I want to ask a follow-up question in that regard, Jeff. With the collaborative effort that took place when the Conficker threat arose, part of the effort there was a public relations effort.

There were public relations people that were brought into the fold. I'd like to ask you folks, you keep talking about transparency. Obviously, that's important. How do you balance the benefits of transparency with the threat?

JEFF MOSS: One of my concerns is as technical folks we sometimes ignore the Layer Eight problem of politics. So sometimes there are these second order issues where if a technical, let's say a name server fails, technically okay, there's a fix for that.

But what are the second order consequences with the political side? If that gives fuel to a certain group that says you're doing a good enough

job, we should probably move that to another forum where we'll take it more seriously.

While that's not directly addressed in your question, there's these one degree off or one angle off situations where you might think, "Well, it's a technical problem. We don't need PR people." But in the end it actually was very useful.

PATRICK JONES: One of the things that we're involved in is actually a cross sector effort to try and educate consumers more on, the interesting point was the health analogy, not just how to keep your machine safe but also how to just have good safe practices in using the Internet.

It's actually got some of the US government involved as well as the browser companies, the ISPs and others. And our thought was even as ISPs we can't solve this alone. There are a lot of companies and a lot of places where we do touch consumers and they just maybe have not been adequately informed.

I think a lot of frustration on their part is just give me the five things I should be doing. And that's not an easy thing for all of us to articulate to them. If you're going to tell them to take some action, that's not always clear exactly what that is and how effective it will be.

BRAD WHITE: Paul?

PAUL TWOMEY: I think the political processes value transparency around process. And that's because they've loaded over a long period of time. So if you take the conflict example, or any other, there's inevitably some part of the dealing with the crisis where frankly a degree of privacy and not being transparent about what you're doing today or tomorrow is important when dealing within adversary.

But what's important is for people to feel like that they know what the process is that's going to be followed, that that's been transparent beforehand. And that there're mechanisms for interacting within it and they do want to see PR and communications take place at an appropriate level.

I think there also needs to be transparency in who's engaged and how's involved and who supplies, and this isn't my general call. I mean this isn't just about conflict. I think this is about all of the ICANN communities' interactions around DNS and DNS security. It's thinking that through.

Because this Layer Eight problem, it's just going to get worse. And with due respect to sort of the engineering type response which is like we'll sit around and talk about engineering issues and sort it out ourselves, that's a spiral downward.

It's not a spiral upwards. That won't be an acceptable answer in a time of crisis. This distinguishing transparency of process and mobilization is different than transparency during crisis itself.

BRAD WHITE: Debbie.

DEBBIE MONOHAN: I think too though we've got a responsibility to try to find solutions even amongst the issues. It's like taking Confecker for example. The approach in dot en zed is…

BRAD WHITE: Debbie, lower that mic just a little bit. We're barely hearing you.

DEBBIE MONOHAN: The problem, the way we did it in dot en zed is that we actually blocked the registration of names that were on the list. But then we set up a solution, a process with the registry and the registrars that, in the case of a legitimate registry and actually one from one of those blocked names, we had a way of actually releasing those and actually seeing the process through.

So I think how you handle it is actually a key aspect. We could have closed everything down and said no, go away. But I believe we still have a responsibility to keep running our ccTLD in a way that actually suits the registrants. So I think knowing what the issue is, there are quite often solutions that can be found in innovative ways.

BRAD WHITE: Yeah, Dan?

DAN KAMINSKY: I believe the focus of PR for anything doing with security has to be an action. You can't just announce something is bad. If that's what you're

doing, then you're I don't want to say wasting people's attention, but you're losing an opportunity.

The time for PR in security is when there's an action that you want people to take to make the Internet a safer place. Like if you don't have a direct action, do this, install that, build this, if you're just informing, I think that's not the best use of time.

BRAD WHITE: Being proactive other than reactive.

DAN KAMINSKY: Don't just announce, look at this big problem. Don't even say, "Look at this big problem that we're working on." I think the most valuable PR in security is look at this big problem, here is a thing that you can do.

Here is, if you agree with what we are saying, this is the action to take. I believe you have to focus on actions. That's my own bias.

BRAD WHITE: Jeff.

JEFF MOSS: I just want to make a quick comment here. I think we need to do that with governments as well as consumers. I think there's a tremendous amount of fear and anxiety about cyber security but frankly they don't know what to do. And their inclination is probably going to be wrong in some instances.

So maybe what the technical community and those who operate the infrastructure, we haven't done a good enough job articulating where can government help? What can be the role? What are we already doing that you don't need to do?

Articulating that more, but I do agree with Paul that I think the risk is growing. The level of concern is rising and they're going to start to take some actions that will be a concern. So I would just add that we should put them in that category of giving them some action.

BRAD WHITE: Sir.

RICK WESTON: I think that it is very important that we learn from other industries on how to react and I disagree with you, Dan, wholeheartedly. Look at any health problem that we've had in the world since we've learned how to wash our hands.

Look at AIDS. AIDS was a problem and it was discussed for many years before we learned how to assault it. Think about any disease that we've had. Look at genetic engineering and the way that we're dealing with health and gene.

Take those as ways to deal with it, very similar situation. We have global problems. These are not our lands anymore and they affect entire populations. That's a different approach.

DAN KAMINSKY: Heath is an interesting analogy and the thing I like most about it is it is non-confrontational. Health is obviously something we all want. But it is a different class of problem. We banned bio warfare pretty much.

It's a technical thing that's possible. We could be exploiting other people's genes, other people's bacteria with viruses, we just don't do that. But, in security, oh no, people are sending out crazy code all the time. So it's a different class of enemy.

RICK WESTON: Okay, we'll have a beer over this later.

BRAD WHITE: Sir, you've been waiting a while. I appreciate your patience.

MIKEY O'CONNOR: Thanks. My name is Mikey O'Connor I'm one of the Co-Chairs of the DSSA which is the DNS security and stability analysis group. Many of you know the genesis of that, I won't go there. I like a lot of what's going on in this room.

I love Steve's kind of throw away comment right at the beginning. Let's not describe what ICANN doesn't do. Let's describe what ICANN does. I love Paul's coordination transparency; think this through in advance stuff. I love anything Dan says.

I want to circle around the document that's in the setup materials for this meeting which is the revised Statement of Remit for ICANN. I don't

love that so much. I think it's, I'm a member of the ISP Constituency and I wrote a long cranky thing.

I won't repeat that either because it was three times as long as the Statement of Remit. But I think we've got to get better at sharpening that up.

I think the role of Remit in ICANN, the fuzziness in there is all the way up at the bylaws there's things like, "What do we mean by ensure?" because you can say ensure in a lot of different ways.

It's certainly not something we can hash through in a meeting like this. But I love the fact that we're having that conversation. I would encourage an upward view.

I know that the tactical technical issues are really important but we've also got to start figuring out how we work together. Who does what in the DNS ecosystem? Thank.

BRAD WHITE: Let's follow up on that. Are we defined by a lack of clarity at this point? Jeff, you're leaning back. Did you have something to say?

DAN KAMINSKY: I think Jeff said it all. He said, "I'm not taking that one." I think Mikey's point is right that the words in the bylaws are perfectly sensible for the time at which they were written. I wasn't there and wouldn't take part in it.

But I imagine that they felt reasonable and if one had asked more detailed questions they would have been "Well, let's see how this works out." Or "Leave it to the details." And now it may well be time to revisit and provide better shape to all of this.

And as I said earlier, ICANN isn't the sole operator in this space. There're a lot of other players, governments of course, industry, what we traditionally call the iStar partners, the regional internet registries, the ITF, the Root Operators for sure.

ALEJANDRO PISANTY: Good afternoon my name is Alejandro Pisanty. I'm from the National University of Mexico, UNAM, and the Internet Society Chapter of Mexico, ISOC Mexico. Can you hear me well?

At the beginning of this year, Jeff Brueggeman who is on the panel, Simon McCalla who has already come to the microphone, and myself, together with a great team of other people from all stakeholder groups delivered to ICANN the Stability Security and Resiliency Review.

Some of the measures proposed there we already see being implemented which was for me very plausible, very good. I don't see the discussion today grounded as far forward as we would like to see.

For example, instead of speaking only of security and attacks, actually speaking of a more integral picture of risk management, which we very much insisted upon. The difference that would make, I mean this is not come back and complain guy who didn't do what I wrote or that I was a part of writing.

But that the discussion could be taken several steps forward. ICANN is put in a situation of asymmetric warfare or asymmetric conflict or engagement in many ways. One of them is that everybody wants ICANN not to do something until something happens.

Then almost the same people will look at ICANN and say, "Who was asleep at the wheel at ICANN and why?" because that's the reason this happened. So you have a massive DDOS against the DNS servers.

Just to pick on the example that Dan especially has been insisting on. You have a massive DDOS. Well ICANN is supposed to not interfere with ISPs, with CCTLDs, with registries, with nobody in preparing for that because everybody is a single independent factor in the multi stakeholder model.

The moment a DDOS puts a couple of Root Servers down to their knees; even if they are one man operations and I think which was expected to bring them down to their knees. There will be an outcry. Where was ICANN and why didn't ICANN prepare for this?

So I think I would hope to hear some report and progress on that kind of stuff. And to make it very concrete in risk management at all layers, including political levels, I think that we should look at. And I would love to hear some opinions from the panel. How much has the risk increased for massive mischief?

I won't concentrate only on the DDOS but also on other stuff including political damage to ICANN or its more visible allies or assumed allies. How much has this risk increased over the last weekend with the US Dept. of Defense announcement with Cyber Pearl Harbor scenarios.

How much does that announcement alone spark the interest of a group? Who would like to at least test the infrastructure for its resilience?

PATRICK JONES: So I really like your view of risk management and I believe that's ultimately where this needs to go. One of the things I asked about was what is the expected growth rate in DNS queries, so you sort of have a baseline.

If we're not growing capacity, well just to go back to the DOS example. One of the only ways out that I see is you have to scale. I don't know yet of a better technical solution than throw more bandwidth at it. Throw more any cast instances at it.

I'd love to know a cheaper, easier to manage solution. But, if that's the world we're going to live in, what would normal growth look like? From what I can tell, with IPv6 AAAA record queries, mobile device queries, DNS prefetching to load pages faster for Chrome, or whatever it is, over the last couple of years.

The number I've heard is about a 30% growth rate in DNS queries. Now that's not necessarily against the root but the software on our networks are generating more queries. You're shaking your head. You can give me a better number later.

But there is a double digit growth in normal traffic queries. So if we're not scaling at that rate, we're essentially falling behind. And I don't ever hear a lot of discussion about what the projected growth rates are in the future.

Do we need to plan for a 50% growth capacity per year? And it seems like those numbers would help tie into a larger long scale risk management framework.

But what I hear is nobody talks about these things out loud because they don't want to tell the attackers the limit to their capacity. So it's sort of a chicken and the egg problem.

BRAD WHITE: Jeff?

JEFF MOSS: Just to add to that, to what Alejandra said, I think what we recommended also is that ICANN needs to have the right structure and process in place to deal with that issue.

I think the Board Risk Management Committee is a good step in that direction and our thought was these discussions need to happen you need to have the right people in the room.

They shouldn't be public, but part of it is building it into the way that ICANN operates so that you are having the right process in place to do that too.

BRAD WHITE: Sir.

TOM DALY: Tom Daly, I'm the Chief Scientist at Dyn. We're a DNS operator. I like what the panel has to say so far. I think you guys are focusing in on the right issues. I would like to put the thought in front of the panel that one of the advantages that we do have that is often ignored is the effect of caching.

Going back to the analogy of world health, the nice thing about the 200 gig DDOS across the Internet is that you know it's happening and you know who's sick. You can generally go and fix those people.

I would be curious though if the panel could comment on the new vector that we've seen just in the last six months of attempts on the registries and the registrars themselves.

Because I actually think that's a much bigger problem because within a given population of people you don't know who's sick and who's not sick, like you do in the case of a DDOS.

DAN KAMINSKY: Thank you. I mentioned this a bit earlier. I actually was at a meeting with ICANN a little while ago where I said, "Hey, registrars and registries are getting or going to get broken into and this is going to become a growing problem."

Let me tell you, I was not popular at that meeting when I said that. But it's true. Everything is getting broken into and registries and registrars are absolutely not the exception. There's no magic reason why their Web servers aren't going to get hit either.

And we are seeing consequences of this, the Google.IE break and a couple of others. I'm afraid on two fronts and you actually hit my biggest fear which is yes, you can go ahead and you can do a very visible "I'm going to change this record and everyone can see it changed."

But you can also not. You can also selectively decide if you've broken into a registrar or registry, at least for a registry, for these guys we're going to go ahead and give polluted recorded.

For everyone else, they're going to get the nice and real thing. We've seen this transition happen in the rest of security from giant worms that affect the world to very targeted, what's called Spear Phishing Attacks.

I think that transition, not only are we seeing the transition from a unintelligent denial of service to a break in of registrars and registries, but I think we're also going to see very targeted use of that enhanced capability.

BRAD WHITE: Sir, you look like you have a follow up.

PATRICK JONES: This is it's a well-known problem. The security team at ICANN, we spend a bit of effort under our capacity building umbrella working with registries and registrars that are asking for help, helping them devise policies and procedures to deal with these as well as technology solutions. I wasn't in that meeting but I would not have been upset. It is a known problem. I just don't think there's a coherent industry response. Go ahead.

PAUL TWOMEY: I think we ought to go up a step and think about this very carefully. Picking up Alejandra's point about how ICANN doesn't do this and ICANN doesn't do that and we're all independent actors until the crisis happens. Then ICANN gets blamed. Part of what we've got to pick up is what ICANN is.

Myself and others have contributed to the building of an institution and part of the building of the institution has been building an executive and building a funding and all those good things. But we mustn't forget that the heart of this and you can go back to the late 1990s where we talked about formation of this community.

It was that it was to be stakeholders coming in together and engaging. I think this is a classic topic that would need much more interaction at the stakeholder level about each of them talking to each other and coming to clarity about what is it they want to see.

If there's concerns about what the registrars are doing or not doing then who's talking to them about that or who's sharing it backwards and forward.

Similarly the Root Service Operators, if the governments have got a concern have they spoken directly to them? How do we use the internal process? I noticed Marc was here and I think there's somebody from Portugal in the back but there's not too many government people in this room at the moment, unfortunately.

But I think we've got to, this particular issue worries me enormously. I'm particularly thinking about the crisis events that are going to

happen. If we don't engage constituency to constituency about what's our common view about this, what's our common approach to this, what's our common approach around transparency and process?

If what we finish today and elsewhere is simply to say, "Well, Patrick and his team should go and do x." we've completely missed it. I think the reason engagement's necessary is there needs to be a common sense of what is this modest stake, truly modest stakeholder and truly transparent approach to it.

Because when the crisis happens, as Alejandra points out and the blame starts going around, there needs to be a "this is the pathway forward we have all agreed." Because otherwise the alternative, you know, everybody loves Plan B.

Right, when the crisis takes place everybody loves Plan B and if it becomes clear that Plan A didn't work, it's that bunch they're useless, there will be a Plan B. and we'll all get broken in that process.

(Inaudible) is talking in this email in this speech about a Cyber Pearl Harbor or a cyber-terrorist attack which could be worse than the thing, in terms of impact on the United States, than what happened on September 11.

Let me point out to you, after September 11, the United States community paid one trillion dollars to go to war. These events can have really massive change pendulums. I hope we keep this dialog going in a way which is about the stakeholders talking really practically to each other about what the common view is, not just what is it we think this (inaudible) is going to do.

BRAD WHITE: Debbie?

DEBBIE MONOHAN: I made the point earlier on about the coordination role of ICANN and that ccTLDs have got a role to contribute here. A lot of ccTLD registries have taken and spent a lot of money putting steps in place to protect their registries from attack and other such things.

I'm aware also of a number of ccTLDs putting in place great security policies in things to actually try and protect or make sure that the registrars systems are protected.

At our own .nz we've employed a manager of security policy and he's going to be identifying the registrar's gaps at the front end. Because between the registrar and the registry that those technical things and those standards are well and truly set in any issue of vulnerability, and they're not allowed into the registry.

I think we need to put it more at the front end as well so that the front end of the registrar systems are okay. And I know that we'd be keen to contribute what we learn and also learn from others.

So when you talk about ICANN I talk about ICANN community and all the range of stakeholders because I don't think anyone's got any one person has the one answer.

And I'd like to be able to pick and choose what .de has done or what .uk and perhaps .com or whatever. And cherry pick the best things of those

to get the optimum solution for .nz. I think ICANN to me has a role and actually coordinating that exchange of information.

BRAD WHITE: Paul, let me follow up on a point you said. You made the note that there are very few government people in the room. In your travels and your interactions with government officials, governments tend to be reactive institutions, not proactive. How do you get that level of engagement where they will come to the table, where this will be on the radar?

PAUL TWOMEY: Well, one thing this happened frankly in the last several years, there's been this quiet dialog going on among governments about the whole cyber security cyber warfare thing.

It gets occasionally comes to the surface and there's been key voices trying to say to them don't throw out the baby with the bathwater. Be very careful, the middle layer works in a different way, be careful about it.

That voice needs to take place but it can't be relied upon and frankly a single generation of people that had that experience who have stood on the system. There has to be the community and the GAC's a key part but there's not just that, the GAC.

There has to be stakeholders have to be a voice saying we're doing the following things and get that message out and be a voice in every country. I take very much the point about the information sharing platform and capability of this community.

CATH GOULDING: Hi. I'm Cath Goulding from Nominet. I'm very new to this environment but I'm not new to the cyber threat. So apologies if my question seems a bit basic. But I'm used to sort of seeing a National News Registers where it might be the threat from terrorism or even a volcano in Iceland grounds or the airplanes in UK for a time.

So there's a National Risk Register and that's quite comprehensive. There's also a cyber-security strategy that's starting to feed into that. For me it seems ICANN and the Root DNS is an international threat. There is no international risk register.

So for me I think a great place, and I don't know, is there a risk register for the Root DNS? And if not, would that be a good idea to feed into governments to put into their National Risk Registers?

[background conversation]

BRAD WHITE: Steve, are you running from the question?

STEVE CROCKER: No, I'm, with apologies I've got to be elsewhere.

PATRICK JONES: Well, I want to wish you a happy birthday, Steve.

STEVE CROCKER: Thank you.

BRAD WHITE: Dr. Crocker turns 17 today.

PATRICK JONES: So there are on the route there are exercises and there is games around contingency planning. There's quite a lot around the root. But remember that's not the Root Operators.

That's just the VeriSign, NTIA, ICANN root. So what the individual Root Operators do is what the individual Root Operators do. It's sort of like you've seen one, you've seen one.

JEFF MOSS: So from the perspective of someone who breaks into stuff, the root's awesome but it's too big.

PATRICK JONES: Big in what way? Too many entries?

JEFF MOSS: The root is not, when I think where is somebody going to attack the DNS, I actually don't think of the root for a number of reasons. One, they're actually incredibly well hosted and there's not that many of them. Because of caching, not every request passes through them.

I'd way rather break into VeriSign servers than break into roots, like the Com Server specifically. There are things you can only say as the hacker

in the room. But no seriously, when I worry about what is someone going to attack in order to impact the DNS, the root is a sexy target.

It's an interesting target. But it's not the primary target. The primary targets are going to be name servers for individual organizations that I want to impact or the registrars or registries that are backing up those name servers that are literally sending other systems to those particular machines.

That's where you have less attention, more exposed. Think about the services that the root services expose. They expose root DNS and generally that's about it.

A remarkable amount of name servers on the Internet today host more than just DNS and once you get into the registrar and registry side, you have the entire Web security semi-fiasco to worry about. So, that's kind of my perspective on the issue.

AMY MUSHAHWAR: Hi. My name is Amy Mushahwar. I'm with Reed Smith and I represent the Association of National Advertisers. Most certainly at this stage we haven't vetted a security policy through our advertisers.

But our group does represent a wide swath of national, US, and International brands and we want it to be on the record that our brands are extremely concerned about security.

However, they're concerned not so much in the infrastructure status and not so much in understanding when a particular hacker Denial of Service has occurred.

What we're really more concerned about is kind of the greater return on investment in that you can use the DNS itself, use the very few protections that we have in place with trademark protections, and spoof names with no breech whatsoever.

We are looking at this that the security team should be working with the BC and the IPC we hope and developing greater rights protections for New gTLDs.

Because of course we're always concerned about the hack, but where you can have a return on investment absent a hack, we really need to be concerned about that as well.

BRAD WHITE: I'm getting the cut signal over here so it looks like we've run out of time. I think what's interesting is almost every person here has talked about the importance of stakeholder involvement in discussions like this continuing. So perhaps this panel, or a panel of this type, can occur at the next meeting and keep occurring as this dialog continues.

PATRICK JONES: Can I ask, by show of hands, how many people thought this panel was worthwhile? And so how many people think we should continue this on an every other meeting or every meeting basis?

Okay, that means I'm expecting you guys to ask questions at the next one. And I'd just like to say a lot of us were here for the whole conference and I'm especially approachable.

If you have anything you want to say, maybe privately, to us or the security team. I'd love to talk to you. So thank you very much for participating.

BRAD WHITE: You folks have been fantastic. Thank you very much.

[End of Transcript]