SINGAPORE – At-Large Workshop: TOR and Alternative Naming Mechanisms to the DNS
Monday, March 24th 2014 – 17:00 to 18:00
ICANN – Singapore, Singapore

HEIDI ULLRICH: Hi, Dave, this is Heidi. Could you go on Jabber, if you have a chance, please? Okay. No problem.

EVAN LEIBOVITCH: Okay, good evening, everybody. Good early, early morning to some of you. Thank you very much for coming here. I realize that it's getting very late in the day, and as it's been said in another forum, I don't want to sit between you and the gala.

We've got what I think to be a very, very important subject to deal with here. By the way, my name is Evan Leibovitch, I'm vice chair of ALAC, based in Toronto and I'm your host and cat herder for today.

When we get involved in talking about the gTLDs and domain names and things like that, sometimes people inside the ICANN bubble lose track of alternatives and other approaches that allow people to get to the information they want on the Internet, so this session is intended to provide an introduction to this.

We have two speakers today. A third, Patrik Fältström, was unable to attend because of the way that today has just gone crazy, and so there's been double and triple bookings. I'm happy that you've chosen to come here, and hopefully we can inform each other. Certainly, I'm here to learn things myself.

So without further ado. We don't have slides for this presentation – well, we have two presenters, and we have slides for the second presentation.

Going first, by way of introduction, speaking form North America where it's the middle of the night right now – so thank you, Dave – Dave Piscitello is Vice President of Security and ICT Coordination for ICANN, and is going to give us an introduction and start to give us a background on some of the concepts behind on this subject.

So, Dave, go ahead. There are no slides for this, so just please listen. Go ahead, Dave.

DAVE PISCITELLO: Thank you, Evan. [inaudible]

EVAN LEIBOVITCH: We can hear you fine.

Okay. Without further ado, Garth Bruen is Chair of the North American Region of At-Large, has been tirelessly working on behalf of At-Large in terms of compliance issues and that kind of thing.

Garth, you have slides for us, right? Okay, so are they ready to be queued up?

GARTH BRUEN: Gisella, thank you. If we could go to the first side that says, "Why this session?" We've already covered some of the basics here. One more. Thank you. That's okay.

I am Garth Bruen, Chair of NARALO. I actually pushed for this session. One of the reasons I wanted to have this discussion is because this discussion was not occurring here. The reason why it was not occurring here generally is because the structures that we're talking about today are not operationally or contractually part of ICANN. There are other peripheral reasons that we'll get into for why this hasn't come up at an ICANN meeting.

I feel it's important that we do talk about it, because they're out there. I'm not going to make any judgments in this discussion, good or bad. We're just going to put facts on the table. Next slide, please.

So, we have to be able to create policy. We have to be able to make informed decisions. One of the facts that we need to make decisions with in-hand is that there are hundreds of other alternate naming systems out there.

If ICANN wants to reach everybody, we have to wonder why these alternate systems are needed. Some people think they're a threat, some people think they should just be ignored. I think that we should discuss it. It's very important. Next slide, please.

Conceptually, the DNS, which is the primary focus of ICANN sessions, is not the entire Internet. It's actually a very small part of it. The IP space is the larger part. And what is the web enabled set of the DNS that actually has content is an even smaller portion.

So, what's really going on in the rest of the space out there that does not have domain names in it? It's actually very interesting what's going on. Next slide, please.

Three main topics: other structures, dotless domains, and Tor domains. Next slide, please.

In terms of alternative routes or alternate TLDs, there's at least 400 or more non-ICANN TLDs out there in operation. There could possibly be more. The ones that are documented are the ones that are documentable. What I mean by that is that these are the ones that have been published or discovered for one reason or another. Two people or a group of people could create their own TLD and just have their own protocol for talking to each other, and nobody would know about it.

Some examples is the Cesidian route is over 100 TLDs. Space.name is over 90 TLDs. New.net is an example, and this entity actually sued ICANN. I'm not sure what the status of that lawsuit is. There are many, many smaller ones like New Nations, OpenNIC. Then there are some defunct ones that did not hang around – eDNS, [Dipperdome], AlterNIC, and Open RSC. Next slide, please.

So, why do these alternate spaces exist? There are different reasons for them. Dot-space, they don't feel that ICANN serves the public, so they want to create their own space. Cesidio, a political independence, it's a non-existent sovereign entity that wants to have its own domain space. Not accountable to anybody. Dot-bit is a part of an economic experiment, tied to the Bitcoin payment system, which is, in and of itself, an alternate virtual currency.

Then there are examples like dot-jack, which was created by a gentleman when he read the Network Working Group their memo expressing concern over alternate routes. They were saying that

alternate routes were bad, so this guy created his own TLD to say, "Well, I'm just going to do it if they don't like it."

Then, of course there are examples like dot-pirate, which is explicitly created for transferring, censorship-free, downloading, and materials. Next slide.

Something that the SSAC addressed specifically: dotless domains. What's a dotless domain? It's exactly how it sounds. It's a domain that doesn't have any TLD extension. Some people would hear that and say, "That's impossible. How could a domain not have a dot?" It's really fairly simple. There's a table where it's tied to an IP address. It doesn't need a dot. The original ARPANET hosts or nodes did not have any dots. The host names existed before the dotted domain system cam into existence. Next slide, please.

Tor "domains" – and domains is in quotes, because the usage of the word doesn't always get approval from everybody. Because Tor isn't actually a DNS in the way that we usually think of it. However, the system does issue unique identifiers that some people refer to as domains. But, these domains cannot be reached in the domain name system.

They are also called "hidden services" within the documentation for Tor. There's an example of what they look like. They usually end in dot-onion. They can only be reached with a Tor browser. The system itself, while not a DNS, operates more like the early host file type system. Next slide.

However, we're going into this discussion slightly backwards, because Tor is not primarily for naming. Tor is a system that adds routing layers to obscure the traffic. It has other security protections in there to preserve anonymity.

In general, it runs counter to the way that the Internet is supposed to work. In the regular Internet, you're supposed to find the shortest path possible, and store lots of information to make communication easy. Tor does the opposite. Next.

This is an actual chart, an example that's pulled from the Tor documentation, where it creates arbitrarily longer routes in order to obscure beginning and end points and the points in between. And, as you might imagine, you end up with something that can be quite slow. People who use it are trading speed for anonymity. Next slide, please.

There's a question out there about Tor being just for criminals. There's certainly a lot of news out there about what are called "dark markets," especially one called "Silk Road." This has captured a lot of media attention, and it's also been kind of attached to the Bitcoin rollercoaster. However, what's going on in this space doesn't reflect the Tor community. And, as Dave pointed out, crime is a problem on the regular DNS, too.

Who uses Tor? Tor is used by activists, journalists, victims, law enforcement, and anyone who wants to preserve their anonymity and have an extra layer of security. Next slide, please.

I've met with representatives from the Tor project. I asked them, "What do you want people to know? What do you want people to take away?"

And one of the things they want me to tell everybody is that Tor is a community. It's made up of people. They maintain the software and they maintain the network, and it's donation and volunteer driven.

It's not intended to replace DNS. What they're trying to do is provide extra security for people who need it. There are lots of different people who need it for different reasons. Next slide, please.

So, with this really, really brief overview in mind – I mean, these are very complicated subjects – there are a number of problems.

There's consumer confusion. There are collisions. Consumer confusion and collisions are tied. It's where you have TLDs and domain names that are the same or similar. One is where the user has a problem with it. The other one is where there's an actual, technical problem.

There are of course legal issues. There have already been lawsuits in this space where the creator of an alternate system with their own set of TLD extensions is claiming that ICANN's creation of new gTLDs violates their earlier claim on those names.

There are, of course, security issues involved, and then there's the ongoing question of governance. Next slide, please.

There are maybe strengths and weaknesses of alternate systems. Certainly, with some of these alternate systems, there's no money changing hands. The access, the domains, are free. But that's not the case in all of the systems.

In some of these systems, there are no owner records. I mean, certainly, that is appealing for some people. It's not going to be appealing for

people who are concerned about crime and trademark violations. But, some of these alternate systems have set up their own WHOIS servers and do collect records.

But then, of course, we have questions about accountability, questions about resiliency of those networks if you're using them, and questions about security on those networks if you're using them.

Certainly, we have our own complex problems in all of these areas within the regular DNS, but at least we have this body and this forum to meet and discuss these issues. This may or may not exist in alternate systems. Next slide.

The motto that we've been hearing for a while is, "One world, one Internet." Can we really say that? Now, these are sort of just questions for thought. If it was necessary for some unforeseen reason to stop an alternate system, is it even possible? Conceptually, are alternate systems and innovation an imitation?

Then, a question in general for domains as a concept: will they even matter in ten years? Will they be replaced by a new layer, or something which just functions better for the end user? So, will this be a non-issue?

With that, I want to turn to the discussion and other people's ideas or problems. Thank you.

EVAN LEIBOVITCH: Thank you, Garth. We'll get into Q&A. Please identify yourself before you speak. Speak slowly. I believe we're still being interpreted into

multiple languages. It also means if you wish to speak in Chinese, French or Spanish, you have that option. There's headphones in front if that's the case.

I would just like to start off with one question of my own before going to the table. One thing that I'd like either of you – or anybody else at the table – to address is the issue of accessibility. Right now, even a number of the new gTLDs are having problems being accessed through browsers.

How much of an impediment is it to be able to use some of these alternates? Do they all require some kind of browser plugin or are they even more difficult to use than that?

GARTH BRUEN: Some of them require their own configurations and even software, but some of the alternate packages out there access all the alternate stuff, which is interesting. It's a big space and requires some exploration.

DAVE PISCITELLO: I'm not certain. [inaudible]

EVAN LEIBOVITCH: Go ahead, Dave.

DAVE PISCITELLO: [inaudible]

EVAN LEIBOVITCH: You're breaking up a bit, Dave.

DAVE PISCITELLO: [inaudible]

EVAN LEIBOVITCH: Okay. I have queue starting. First, Alan, then Eduardo. Alan?

ALAN GREENBERG: Two comments. First, to address Garth's last question of what will be there in five years or ten years? Will the current DNS and domain names be relevant?

There's a very longstanding gestation period for technology, with very few exceptions. The time it takes from the time to demonstrate something in a lab environment until that it becomes reasonably widely accepted tends to be about eight years. It's been like that for 30, 40 years. There are occasional things that bloom a lot quicker, but not very many.

That means, when you try to predict what's going to be the "in" thing in five or six years, it's already around. The challenge, of course, is picking which one. So I'm not going to try to pick what will be – will the DNS and domain names as we know them today be the right things five years from now or seven years from now, or will something be on its way up in place? The world is far too complex, there's too many variables to predict, and I certainly wouldn't try to make any money on it.

You don't have to go as far as Tor to look at things that do their own routing and have their own lookup. Skype, especially before it was rewritten after Microsoft took it over and before they rewrote it to work well on mobile devices was essentially a world unto itself.

If you happen to have a computer with multiple connections on its two different networks, Skype might very well have used your node as a bypass to skip from one network to another. It would decide how to get the best place from you to your other people. Of course, it uses its own naming system, completely outside of the DNS. A very common thing that we're all using, but we're not threatened by it.

There's a lot of things in this world that are potentially dangerous, and if everyone tried to build their own Skype system and stop using the DNS, we would probably have a real messy system. But as long as one or two only do it and they do it carefully and without too much error, you live with it.

EVAN LEIBOVITCH: Go ahead, Dave.

DAVE PISCITELLO: I think that [inaudible].

EVAN LEIBOVITCH: Okay, all right. Next, Eduardo.

EDUARDO DIAZ: Thank you. I have a question about the Tor network itself and how is that in relation to the – well, we have heard about the NSA doing spying on the Internet. Does that include the Tor network? Can they spy through the Tor network?

GARTH BRUEN: Sorry, I was talking to Gisella about an offline remote question. Just repeat that, Eduardo.

EDUARDO DIAZ: Yes, Garth. Basically, with this news about the NSA spying on the Internet, does that include the Tor network?

GARTH BRUEN: That would include anything really, first of all. It's a complex history, because the U.S. government had a hand in creating Tor. It was created in a Navy lab, and it's still absolutely used by various government agencies, and now government agencies all over the world. And I think Alan has a very specific response to that. Go ahead.

EVAN LEIBOVITCH: Alan, go ahead.

ALAN GREENBERG: Two parts. I keyed in on when you said "recently discovered." I remember a discussion I had with some senior network engineers, 1995. That would be 19 years ago. We were talking about what were then the main hubs in the U.S. –MAE-East and MAE-West – and each of them had

a big cable and a room beside them, which was used to capture all the traffic for the government. Not exactly new.

But, to answer the specific question, it's running over the IP network, it's visible in the main hub routers. The only question is, to what extent can they recognize the traffic and decode it if it's encrypted? There's probably a good chance they can.

NIELS TEN OEVER: This is Niels ten Oever from Article 19. I think we have to be a bit more precise here if we're talking about Tor. There have been very explicit slides from the NSA that show that the NSA cannot filter traffic from Tor. There have been direct implants into an old version of Firefox through which they, upstream, have tried to target Tor users. But, this was not a large group. Before the patch came out, the zero day, it was already patched by the Tor team.

The NSA slide itself say that for them, it's impossible practically to break Tor. There is the theoretic option of the timing attack where the NSA would filter and fill up the whole network. And then by timing correlation attack, seeing where the traffic is coming and from, and thus de-anonymizing the user. But, for that, they would have to monitor the whole network in near real time.

We don't think they have the capabilities of that yet. So I think we should say that, if one wants to be anonymous on the Internet, Tor is the best option.

EVAN LEIBOVITCH: Having said that, I think that we might be mindful of the fact that there have been times in the past where the NSA has told us they don't do things, when in fact maybe they have.

So I understand what you're saying. It's just simply because the NSA has slides saying they can't do something, I'm not necessarily sure I would believe it.

NIELS TEN OEVER: I would come back to that. The NSA did not tell us this. We found it out because Edward Snowden chose to leak it.

And I'd also like to react to what was said about the money going into Tor, and that it was developed in Army labs. No, It was developed by Roger Dingledine with funding. That is really something else than being developed internally by the military. The military never had any say over the code. It has always been open-source, it has always been researched and based on best practice cryptographic protocols. So let's not insinuate something that's not the case.

EVAN LEIBOVITCH: Thanks, Dave. Next question comes from a gentleman who put his hand up, who is now handing cough drops to the audience. You're next. Please identify yourself.

WARREN KUMARI: I'm Warren Kumari. Unfortunately, I arrived late, so if this has been covered, feel free to stop me.

So, one concern with alternate naming schemes is the possibility of leaking into the DNS. This is things like for the onion stuff, for example. If you e-mail around a link to an onion type URL, somebody who doesn't have the browser installed will click on it and have issues.

So, there's a draft that myself and Andrew Sullivan have written in the IETF which discusses ways to mitigate this. Basically, when people are using or recording DNS-like names – basically labels separated by dots, which is the easy way to do stuff, because you want them to work in browsers, etc. – when people are using these in a non-DNS context, we've got some advice on how to do this safely.

Also, we're suggesting that a label be reserved to denote that this is an alternate name space. So, basically, if you're using an alternate naming scheme, you put a label at the end of it to signify that this is different in the DNS context.

The draft is draft-wkumari-dnsop-alt-tld, I think. If anybody is wildly confused at this point, I'm happy to chat about it afterwards or answer questions.

EVAN LEIBOVITCH: Could I possibly ask you if you have access to the Adobe Connect to type that in, or at least to give somebody here the ability to put that into the chat so we can get that link? That would be great.

Okay, next in the queue, I have Garth and I have Gisella Gruber, who will be reading something from the Adobe Connect room. Garth?

GARTH BRUEN: Thank you. I just want to go back to a point earlier about Tor security. A question for the folks from Article 9, or really anybody. Do you have concerns about exit nodes and the security of exit nodes?

NIELS TEN OEVER: There have been several papers and theoretical papers and also research lately done about possibly compromised exit nodes.

In the threat model that was earlier shown, it is clear that traffic inside the Tor network is encrypted between the nodes, but it's not encrypted from the exit nodes to the final traffic. So, indeed, it is possible that law enforcement agencies or other third parties could host an exit node and thus capture the traffic.

But it would then still be hard to lead it back to where the traffic is coming from. So, indeed, it would be possible to sniff traffic, but it would be very hard to find it back to where it's coming from.

Then, one would have to use browser exploits, and that's why the Tor browser comes with no script and other additions, which makes that much harder. So, yes it is an issue, but not necessarily to de-anonymization.

GARTH BRUEN: Just so everybody else understands what we're talking about, from end to end in the Tor network, you don't see who you're talking to or you don't know where they are, but the person immediately ahead of you does know. That's the exit node operator.

EVAN LEIBOVITCH: Dave, do you have anything to add to any of this?

DAVE PISCITELLO: No, I think [inaudible]

EVAN LEIBOVITCH: Okay. Next in the queue is Gisella Gruber, who will be reading comments from the Adobe Connect room.

GISELLA GRUBER: Thank you, Evan. From our remote participant, we have a question from Poomjit, member of NCUC from Thailand: "I'm curious to know which chat application is currently most secure for the users and or activist journalists, especially for the activists who have to work and live in tense political crisis." End of the question. Thank you.

EVAN LEIBOVITCH: I'm not sure if that's totally applicable to this subject, but if anyone's got any quick recommendations, either we can put it back in the chat room so that our friend can find out.

I know that I have a couple of apps that do secure chat, but I think many people sort of have their own. Short of just going around the table and asking everybody what they use, I'd rather if you have something, please put that in the online chat to assist.

Are there any other questions that anybody else has? We've got some very good skilled people at the table here, so here's the time to ask.

I just wanted to add one point on my own, and that is to remind people that there is a gTLD Metrics Working Group that the GNSO created to try and gauge the amount of consumer trust and choice and things like that stemming from the new gTLD program.

One of the things that the ALAC has tried to do is to make sure that the metrics don't necessarily just say, "Okay, there's greater choice because now you have this many hundred TLDs instead of just having a couple of hundred," but we also wanted to make sure that the metrics are also gauging the popularity of the DNS, related to alternatives in the possibility that if there is consumer confusion relating to this massive new influx of gTLDs, is this going to lead people to alternatives? Is it going to lead people to Tor? Is it going to lead people to more use of mobile apps and QR codes and social media, park pages, home pages, and things like that?

That's simply something to note in terms of alternatives. Along with me feeling my age because I'm now harkened back to some of my UUCP days, listening to some of the table instances. The use of dot-onion reminds me a little of the old UUCP pseudo top level domain.

Garth, you had something to add?

GARTH BRUEN: Just in general, I want to try and see if we can keep doing this in future ICANN meetings and we can develop this discussion better. I had asked people form the Tor project to possibly present at a future meeting and expand the discussion on that specifically.

And also, maybe we can actually get a group to study alternate DNSes, specifically. Maybe Dave has some more information on that. Maybe At-Large could publish some information about it. Thank you.

EVAN LEIBOVITCH: So, I would add, as chair of the meeting, we've got some very good expertise here from the looks of things. I see Glen. So, hopefully we can ask some of you to come to us at the end, so we can start putting together this group going forward. Glen, go ahead.

GLEN MCKNIGHT: I just want to follow up on what Garth said. Evan and I are going to be at the IETF in Toronto in June, but also we're organizing a Canadian Internet forum in October. So this looks like a great discussion. We'd like to help facilitate one in June and one in October. If anyone is in Canada, please approach Evan and myself, and perhaps we can further this discussion. Thank you.

EVAN LEIBOVITCH: We have about ten minutes left in the hour, and I can see people fading. I've got two more. Eduardo first, and then a gentleman from our Article 19.

EDUARDO DIAZ: I'm just curious. I mean, I have heard about Tor before. So if I use a Tor browser and I can really browse anything on the Internet, but the only thing is that they will not know where you're coming from. Is that what it is?

EVAN LEIBOVITCH: Could you answer into the mic? This is useful for – we have remote participants as well.

GARTH BRUEN: Yes.

EDUARDO DIAZ: I'm sorry, Mr. Chair. Can I follow up on that? So, if I'm using a browser now, like Tor browser, to browse the Internet, what is this outernet space that we're talking about? Is that that we can reach this outernet space through this browser?

GARTH BRUEN: Well, the outernet space is really separate from the Tor concept. I mean, it's really what you have are alternate system out there that you can't get through the normal DNS. You get special configurations to be able to access them. Tor may be one of the ways you can do it. There are other ways. Tor, for many people, is more about the communication.

EDUARDO DIAZ: Okay. So just to finish up, so we're talking about two things. Tor is one thing, and the outernet space, something else? Okay. Thank you.

EVAN LEIBOVITCH: Okay. Gentlemen, go ahead.

NIELS TEN OEVER: Yeah, it's Niels ten Oever from Article 19 and NCUC. There are two points that might be of interest. So, one thing is that there are also other reasons to use dot-onion addresses, and that is their resilience to DDoS attacks. It's far harder to do that within the Tor network. So, that is a reason to avoid not only censorship, but also other forms of censorship via attacks.

Secondly, what is perhaps one of the most interesting things about alternative domain systems is how they can interact, and therefore I would like to point your attention to a project called Tor2web through which it's possible to reach onion addresses via an intermediate proxy. So that might be an interesting way to link different areas and get the best of both worlds.

EVAN LEIBOVITCH: Sorry, could you possibly type the link for that into the Adobe Connect room? That would be great. This helps us keep a record of that.

Okay, we're near the end of our session. Go ahead, Dave.

DAVE PISCITELLO: Just a quick [inaudible] might want to take a look at [inaudible]

EVAN LEIBOVITCH: Sorry. Dave's referring to SSAC 009, which is one of the SSAC recommendations. Do I have that right, Dave?

DAVE PISCITELLO: Yeah, that's right.

EVAN LEIBOVITCH: Okay, thank you, Dave, and good night. Garth, you've got the last word.

GARTH BRUEN: Thank you, I already had it. That was just that I wanted to continue the discussion in future meetings and think about it.

EVAN LEIBOVITCH: Okay. On that note, we're three minutes to the top of the hour. So, thank you all for coming. I hope it's been informative to you as it has been to me. Okay. So again, thanks, and have a good rest of the conference.

And one last thing. I want to thank the interpreters who are in the back of the room and who have been toiling. It has been a source of pride that the ALAC room has been one of the few that has been consistently interpreted into multiple languages throughout many of ICANN's meetings. The GAC recently got wind of it, and now it's in their room and the main room. But I think we had it first.

And, as well, not only tech support, but also the folks that over here in the corner, our own staff, our own ICANN staff that has been doing everything from writing crib notes for Steve to keeping track of the projectors and everything else that's been going on. You guys keep this thing running.

And, as well, the guys in the back that have made the audio and the projectors work. Thanks, you all. It's been a very long day, and thank you all.

GARTH BRUEN: I also have a small stack of Tor stickers, if anybody didn't get one and you want one. There you go.

UNIDENTIFIED FEMALE: Thank you, everyone. The meeting has been adjourned.

[END OF TRANSCRIPTION]