Transcript
DNS Security and Stability Analysis Working Group (DSSA WG)
8 September 2011 at 13:00 UTC

Note: The following is the output of transcribing from an audio recording of the DNS Security and Stability Analysis Working Group (DSSA WG) teleconference on 8 September 2011 at 13:00 UTC. . Although the transcription is largely accurate, in some cases it is incomplete or inaccurate due to inaudible passages or transcription errors. It is posted as an aid to understanding the proceedings at the meeting, but should not be treated as an authoritative record. The audio is also available at:http://audio.icann.org/gnso/gnso-dssa-20110908-en.mp3
On page:
http://gnso.icann.org/calendar/#sep
(transcripts and recordings are found on the calendar page)

Attendees on the call:
At Large Members

- Olivier Crépin-Leblond
- Cheryl Langdon-Orr
- John Levine

ccNSO Members

- Jörg Schweiger, .de (co-chair)
- Takayasu Matsuura, .jp
- Katrina Sataki, .lv
- Wim Degezelle, CENTR
- Jaques Latour, .ca
- Otmar Lendl, .at
- Luis Diego Espinoza,.cr
- Ondrej Filip, .cz

GNSO Members

- Greg Aaron – (RySG)
- Scott McCormick
- Mikey O'Connor – (CBUC) (co-chair)
- Rafik Dammak, GNSO
- Rossella Mattioli – (NCSG)
- Rick Wilhelm, Network Solutions

NRO Members

- Carlos Martinez (LACNIC)

SSAC

ICANN Staff:
Bart Boswinkel
Glen de Saint Géry

Apologies:
Arturo Servin (LACNIC)
Julie Hedlund
Sean Copeland, .vi
Jim Galvin (SSAC)
Mark Kosters (SSAC)
Patrick Vande Walle – At large
Chris Wright, .au
George Asare-Sakyi – (NCSG)
Adam Palmer – (CBUC)
Edmon Chung -At Large
Don Blumenthal – (RySG)
Andrew de la Haye (NRO Member) - for the next 4 weeks
Mohamed El Bashir (At-Large)
David Conrad (SSAC)

Coordinator: The call is now recorded. Please go ahead.

Glen Desaintgery: Thank you (Louise). Good morning, good afternoon, good evening everyone. This is the DSSA call on the 8th of September.

And on the line we have Rafik Dammak, Cheryl Langdon-Orr, Mikey O'Connor, Jacques Latour, Scott McCormick, Greg Aaron, Olivier Crepin-LeBlond, Otmar Lendl, Takayasu Matsuura, Joerg Schweiger, Bart Boswinkel, Wim Degezelle, and Katrina Sataki. Keith Drazek has just joined.

And for staff we have, sorry it was Bart Boswinkel for staff and myself, Glen Desaintgery. We also have Rick Wilhelm who has just joined as well. We have apologies from Arturo Servin.

And may I ask you please to say your name before speaking for the transcription purposes. Thank you very much and over to you Mikey.

Mikey O'Connor: Glen we also have apologies from Mark Kosters and...

Glen Desaintgery: Mark Kosters, yes.

Mikey O'Connor: Mr. Blumenthal and...

Glen Desaintgery: Don Blumenthal, yes.

Mikey O'Connor: And let's take a quick look. May have a couple more. I'll check after the call. I think probably some of the apologies went to Gisella instead of to you so.

Glen Desaintgery: Fine. Thank you so much Mikey.

Mikey O'Connor: Welcome all. As usual we'll do first a quick pause to see if anybody has an update to their statement of interest before we get going. All right.

And I think the agenda's pretty straightforward. But I think it will also be a really interesting call today. And I think I'm just going to blend the two big items, which is continuing our discussion of this draft threats document that we've been working on.

But combining it with a discussion of Greg's email to the list. And just for sake of simplicity, I'm going to share it on the screen, if I can pull this off. Let's see. Short pause while I get my on screen back. Can people read that? Is that too small or is that big enough?

That just so happens to have the whole email on the screen at the same time, which I think makes it easier to deal with.

And what I thought we could do maybe is I haven't actually checked with Greg. But I assume that it would be okay Greg if you kind of took us through this.

And then see if there's any sort of violent disagreement with what Greg has to say here. And if there is, let's talk about that. And if there isn't, then maybe use these as sort of rules that we can then start going through the threat document and putting things in piles of what's in scope and what's outside of scope.

So Greg, do you want kind of run us through this real quick? You're muted.

Greg Aaron: Hi, this is Greg.

Mikey O'Connor: Oh there you go.

Greg Aaron: I think their might be some, you know, based on what I said there might be some things that could be completely excluded. And then there are some probably some things that we may want to talk about. But they need to be put into an appropriate context.

What I did in this mail is I quoted a bit from our charter which speaks to the focus of the group, which is natural level of frequency and severity of threats to the DNS.

And when the chartering team got together this was discussed. It wasn't to be about anything that happens through or on the DNS but more about the overall system itself.

And then so it said it should limit - the group should limit its activities (unintelligible) and top-level domains within the framework of ICANN's coordinating role.

So that's kind - that's a reference to the ICANN mission and bylaws. And that's of course on the ICANN Website.

You know, and there's always little discussion that could or should take place about what exactly that means. But this is kind of my attempt to articulate what I think it means.

There are some topic I think which could probably be excluded totally because they don't rise to that threshold. So that would be things like phishing, cybersquatting, operating system vulnerabilities, you know, in Windows or something.

Those are outside of ICANN's mission in a lot of ways. Also they don't threaten the system itself. They don't threaten to bring down the DNS or have a significant impact upon the overall system. They're more to do with individual domain names or individual companies or entities.

And then I had a list of things that were perhaps did rise to that level. You know, flaws in the DNS protocol, alternate routes, those kinds of things.

When I was thinking about this, there are some things on our list which might be very relevant to talk about. But they need to be put into a context. So for example, DDoS is a threat. But most DDoSes are probably not (further) for our group to talk about.

You know, if an individual company is getting DDoSed that's probably not for our group. Now DDoS is a potential serious threat if it's a TLD or a route server that's getting attacked though.

Similarly, you know, a business or a system failure at a route server operator would be a potentially big problem but not at a NISP or a transit provider. So I offer that as maybe a way of putting some of the things in our list into a context.

We don't want to lose sight of those things. And we might want to write about them and talk about them. But we need to make sure of the context in the scope. So those are my thoughts. And I welcome any feedback.

Mikey O'Connor: Thanks a lot Greg. I think that part of the reason I wanted to just do it this way is because I thought that your note was a great one. And I wanted people to actually take a moment to step through it.

Sometimes things go by on the list. And we don't give them the attention they need. Do people have thoughts or comments about this? Go ahead Joerg.

Joerg Schweiger: Hi Mikey...

Mikey O'Connor: You may be muted.

Joerg Schweiger: No, not anymore right?

Mikey O'Connor: Right. You're all set now.

Joerg Schweiger: Okay so this is Joerg Schweiger for the transcript. Actually I would completely agree to what Greg said. But if this is true, what I think what we should do is that we should alter the mission statement we want declared.

And that is due to the fact that we stated a mission statement saying that we want to take a look at the current state of stability, security and resiliency of the DNS.

If it would be just resiliency we look at, then what Greg said is absolutely true. Then there is no need within the definition we took from the (ethic) stability, security and resiliency definition to for example take a look at phishing, spam, malware and whatsoever.

But if we would take this definition, then it might be relevant to take a look at spam and things like that as well. But referring once again to the charter I think Greg is absolutely right.

And if we take it straightforward what the charter said, then we are focused on resiliency and then spam and all the other kind of things he mentioned wouldn't be in scope as far as I can see it.

Mikey O'Connor: Thanks Joerg. I've done something peculiar to your status because Adobe Room put a check mark right in front of me and I checked it. So now I don't know how to undo the damage that I've done.

And so who knows what's going on there. Anybody else got thoughts about this? Olivier go ahead.

Olivier Crepin-LeBlond: Thanks Mikey. This is Olivier. I would agree with Greg based strictly on the framework itself, considering just the top-level domain and the routes level.

However, I do wonder if we shouldn't also look at domain hijacking and cybersquatting, phishing when one looks at the new GTLDs that will be launched, if there is an actual pattern of these things happening specifically in some new GTLDs than others.

I have great concerns that some of these new GTLDs will be used for malicious intent. And certainly it will need to be ICANN's role to monitor the use of the GTLDs in general.

And to find out which ones are the, you know, as opposed to the high security ones. Look at the high rogue ones as such. So I wonder how others feel about this in the group. Thank you.

Mikey O'Connor: Thank Olivier, (John) go ahead. You're probably muted (John).

(John): Oh.

Mikey O'Connor: Here we go.

(John): Here I am. I think the points that Olivier addresses are reasonable ones. But I don't think they're ones we should address. I mean I think that given our limit - given our limited time and non-existent budget and so forth, I think that Greg has identified a reasonable set of threats for us to go ahead on.

And I think we should simply document the fact that we're aware that these other things are an issue. But we're not addressing them. And I think it's a reasonable distinction to make between threats that are essentially technical and the stuff that Olivier is addressing, which are basically threats that are administrative.

Mikey O'Connor: Okay, anybody else want to chime in? One of the things that I especially like about this was the distinction that Greg drew in the final paragraph. Which is I think that what we can safely do is use as our test, is this a threat to the DNS?

And it might be that a DDoS attack is a threat if it's against a DNS related server. Clearly it would be outside our scope if we were talking about DDoS in general, like to Amazon.

And so I think that circling back to the phishing, spam, malware, blah, blah, blah, I would agree that taking on those issues across the board is way outside our scope.

However, it may be that we'll want to kind of keep it on the back burner. For example let's say somebody phished a registry operator. And stole credentials to their infrastructure. And used that phishing attack to gain control of a registry. Let's take a sort of dooms day scenario.

I think in that context we would all agree that that's in scope right? And maybe I'll circle back to Greg for my sort of rhetorical partner here. But Greg would you agree with a kind of twisted analysis like that if somebody phished a registry and got access to credentials to a key system or server on the registry side. That that would be something that would be inside our scope?

Greg Aaron: This is Greg. I'd have to think about whether we would call it phishing or maybe generalize it to something like the compromise a registry. I mean phishing itself is I think pretty clearly outside.

And I'd say that from my experiences in the registration abuse policy working group that the GNSO had. And we talked about, you know, the issue of individual domains.

I mean the compromise of a registry could be accomplished of course several different ways. Phishing is one or (direct tax) could be another. We would probably then want to talk about well what does that mean? What could you do? And is it a - how big of a threat is that?

It's going to depend on a lot of things. And even then I'm not sure if it necessarily rises to the threshold. I might depend on which TLD you're talking about.

Mikey O'Connor: Yes. I sense a fair amount of agreement across the group. Is there anybody, Olivier circling back to you, what's your reaction to subsequent conversation in terms of the point you were raising? Sort of role TLD thing.

Olivier Crepin-LeBlond: Yes thank you Mikey. This is Olivier. I'm - I don't feel so strongly about one way or the other. Generally yes, I know. We need to just focus on the TLD side of things. I know that.

And it's just, you know, when one speaks of the, just speaking to the technical side of things. Or if one should also look at the administrative instability, I would think that the administrative instability has something to do with it as well.

But I may be wrong. I know that it's a lot easier to look for the technical instability of things. The question is, you know, I find it to be linked to the administrative instability as well.

We've seen in the past some problems arising from the administrative instability. So I'll leave it to you. I'll leave it to the consensus. Thanks.

Mikey O'Connor: Well and I think that that's sort of with Greg's point of registry compromise. And, you know, I think there's pretty broad agreement that a compromised registry is a big problem. Well it may not be. But it probably is.

Olivier Crepin-LeBlond: So Olivier here. And this has actually happened. Registries, or was it a registrar's database, one or the other. I don't have the exact points at hand. But has been compromised in the past. And that has introduced a whole lot of potential problems.

Mikey O'Connor: (John) go ahead.

(John): I hate to split hairs, but I think it kind of depends what we think of as stability problems. I mean I'm just trying to think, you know, if we had a registry run by totally evil people.

And if we for the moment assume it's not .com. I'm just trying to think what they could do that would cause instability for the DNS as a whole as opposed to simply screwing up their own TLD. And at the moment I’m not seeing it.

Mikey O'Connor: And this is a question for better minds than mine that's for sure.

(John): I mean I think we might sort of stick that on the back burner to scratch our head about, but for the time - thinking that you haven't given it practically two minutes of deep thought.

I can - I have to say that I'm having, I mean I can see all sorts of, you know, phishing attacks where they can publish a variety of domains with misleading names and so on and forth. But that's not a stability problem.

You know, it's all, you know, as far as the DNS is concerned, you know, those are names and they're being served up. And they don't interfere with anything outside of the same TLD.

Maybe it's possible they could do something evil by pushing glue into other registries. But that's a pretty arcane attack.

Mikey O'Connor: Could they, then this is again the voice of a complete idiot. But could you induce a whole lot of route flapping across the whole DNS if you had control of a registry and you started toggling IP addresses like crazy?

(John): These are domain names. I don't - I'm not really see how they could, you know, I realize they're regis - you know, reg- you know, each registry presumably controls a little network of its own in which they could do various bad stuff.

But that's kind of, you know, but that's sort of - that's the same issue as with anybody and any hostile party controlling a network. So I don't think that's a DNS issue.

Mikey O'Connor: Okay. Any, oh we just lost Greg. Yikes, what have I done here? I completely goofed myself up.

Greg Aaron: Oh I'm back.

Mikey O'Connor: Oh good.

Greg Aaron: Mikey I had a comment on that point by the way. The issue of the evil registry came up a lot of course during the new TLD discussions.

And the main problem that everybody seemed to be worried about was if you own a registry, you can register or allow people to register a lot of domains. Which are then used for bad purposes, again phishing, malware distribution, spam, those kinds of problems.

That seemed to be the focus. I don't recall how a registry operator would really mess with the rest of the DNS system. There might be some interesting arcane ways. Maybe we should not lose sight of that.

But I think the main problem was malicious use of domain names registered within that new TLD. Which is why we have the new requirements for background checks and compliance and all those kinds of things.

Even then though the registry operator doesn't have any direct responsibility for the use of the domains in its TLD. You know, that's kind of down the chain. So there's a - that's kind of the legal issue there.

Mikey O'Connor: Okay. I think then that what I'm at least hearing is that we as a group, with the folks on the call who have had this conversation, are pretty comfortable with Greg's summary and kind of rules of the road.

And so I think what we'll do is we'll post this out to the list and say this is a consensus candidate. We'll follow our rule that says we'll talk about something for at least two calls.

And then if we get through another call on this, either in tact or with minor editing then, you know, we'll move this document into the pile of things that the group agrees on.

And in the meantime what I'd like to do is sort of test it today by going back to our gigantic list of threats and seeing if we can start to use this as a way to categorize things that are on that.

And so if you'll excuse me for a minute while I re-jigger the screen, switch to actual - find map. Now that's better. Okay.

What I'm going to do, I'm going to test something here. Pay no attention to what's going on on the screen at the moment because I just want to see if the thing will work. It does work. Okay.

So what I'm going to do as we go through this is I'm just going to sort of color code things. And, you know, I think I'm going to use a very clever color code. If it's red, we'll declare it, you know, that's the color we'll use to declare something outside of scope per Greg's email. If it's green, it's in. If it's not colored, it means we're still trying to figure it out.

And with that what I'd like to do really quickly is go through this. And it may be that it takes us a call or two to do this. We'll see. And see if we can put these in piles.

Now it may turn out that that gets too slow. We often run into this thing where this tree is so big that going through it item by item on the phone gets pretty tedious.

But I'd like to use a little call time just to test our understanding of where we're at with the scope thing. And then if we're feeling pretty comfortable with it, again I can go ahead and take some time between calls and sort of tentatively put the rest of them in piles.

And then we can review that rather than doing it one by one. But I think it's useful just to test the consensus to go through this one by one for a while.

So starting right at the top with something kind of complicated. Here's the registry business failure thing. And this spans to sort of look like that. And so let's have a little chat about what we think of this part of the list.

Clearly the higher up the tree we can put a red check, the more of it we can eliminate. And thus reduce our scope and become more focused. So is the business failure of a registry, given our recent conversation, which category do we put this in? Is this in scope or out of scope?

And no, I'm not going to do this for you. I want somebody to raise their hand and make a case one way or the other. Greg go ahead.

Greg Aaron: Thanks Mikey. This is Greg. This is a tough one. In some ways I think it depends on which TLD you're talking about. .Com is 45% of the domains on the Internet.

I'm going to have to drop off and get a new phone. Sorry about that, I'll be back with you in a minute.

Mikey O'Connor: Okay thanks Greg. Anybody else want to jump in while Greg is getting back on the conference bridge, anybody responding one way or the other to the notion of which TLD? Don’t all speak at once. Olivier, there we go. Now we got some folks on. Go ahead Olivier.

Olivier Crepin-LeBlond: Thanks Mikey. The notion of which TLD is some - is a point which I think is moot. Every TLD is important. And so the failure of any TLD is going to introduce instability, whether it's a TLD that serves 20 domains or whether it serves 20 million domains. It's a failure.

And so yes, it will - the one with 20 million domains will affect more people than - and more users than the one with 20. But it's still a failure. Thank you.

Mikey O'Connor: Okay. I'm going to capture this comment. I'm going to start doing scope. Joerg go ahead.

Joerg Schweiger: Yes thanks Mikey. This is Joerg for the transcript. Actually everybody else seems to be in favor of taking a look at this point. I do not, and that is all to the fact that I doubt that the failure of any registry, maybe except .com, would have a major impact on the DNS itself.

And if this is the case, I don't see that the business failure would be within our scope.

Mikey O'Connor: And I think that's the point that Greg is making, although he's leaving himself a little bit of room to maneuver on a really big one. Let me just...

Greg Aaron: Hi Mikey. This is Greg.

Mikey O'Connor: Yes go ahead. Jump right in.

Greg Aaron: Yes, .com and .net were in the back of my mind. .Net because there are so many important .net name servers out there. But, you know, and when a TLD fails, what does that mean? And does that mean they stop propagating DNS for example?

You know, eventually the records will expire and look-ups for the domains won't work. Now in a small TLD hardly anyone may notice. And I don't think it affects the overall system.

Common net failure would be, you know, kind of a wide spread impact. What happens when a TLD also fails is ICANN has a fairly defined but limited role having to do with its IANA responsibilities.

If a CC TLD fails for example, ICANN doesn’t have much to do about it unless there's a re-delegation request. If it's a gTLD failing, then ICANN has some procedures for, you know, retrieving the escrow and maybe getting that TLD into the hands of another operator to mitigate the problem.

Mikey O'Connor: Okay. It looks like the queue is cleared. John is agreeing with - John Levine is agreeing I thing with what Greg was just saying. So tentatively what that would imply to me is that we could color this one out of scope like that. Anybody got a serious problem with that idea?

All right. Tentatively that's what we'll do and move on. Good. That's good. I like this. I think this is going to work. Now I'm going to change our focus to system failures. This is kind of a laundry list that came from one of documents that I summarized. I can't quite remember which one right off hand. I can get back to it.

And this could be a nuanced one. It could be one of the ones that we say it depends. Again, I'd like to hear given our current conversation that we had about Greg's email, how would folks like to handle this one? Break it into chunks, eliminate the whole thing, leave it for another day; we could do that too.

You know, it seems to me that if these things happened - I guess the question is if these things happened in a registry, what would their impact be? And it would seem to me that some of them are probably more (impactful) than others. (Yorg) is lobbying for taking this one out unless it's a root server operator. Interesting angle. Any other thoughts on this one?

A lot of people typing but nobody talking, which is fine.

Rick Wilhelm: Mikey, this is Rick - Mikey, this is Rick Wilhelm. I can't find the raise your hand thing.

Mikey O'Connor: It's up on the very top in the center of the screen.

Rick Wilhelm: Oh there it is. Okay.

Mikey O'Connor: Yes. There you go. But I will give you a completely free non-raised hand permission to talk this time.

Rick Wilhelm: Wow. Thank you. So I think it - for all thee things about system failure who really depend on which systems we're talking about perhaps to say the obvious because, you know, there's a lot of things that can go wrong in a - registries are big complicated things. And there's a lot of things that can go wrong and it doesn't matter at all in the short term.

But there's other things that it - for example, if people can't make DNS updates at any one time, it's hugely problematic. And so consequently even when registries do SRS maintenance that they typically have avenues set up to do ad hoc - or spot DNS changes that registrars might need even during an outage of the SRS that normally would preclude such things. So it really depends on what kinds of things are bailing.

Mikey O'Connor: All right. Oh, there's your hand up. Cool. It's working. I'm going to let people take their own hands down because when I click on them, I turn on this microphone thing and I have no idea what that does. And I'm a little worried that that may be contributing to the echo. So I'm keeping my hands off of that button that appears on my screen.

Any other thoughts about - let's see. (Katrina) and Jacques have thoughts. (Katrina) is saying I think it can't be out. Either it's out without any ifs or it's in and it's properly described. I think that's probably correct (Katrina). And Jacques says out and operational failure is not a security threat.

And I think that Rick has pointed us down a fruitful path here which is that if - maybe the thing to do is focus on the impacts of the failure rather than the failures themselves. And that if the failure - and it would perhaps be useful to develop lists of failures that have an impact that do matter to the security of the DNS. And then stratify the rest of this list that way.

And so one way to handle that might be to do this, which is to take - oops. Not that way. Take all of these, put them in a list like that; call that list - and then focus on the impact question that Rick raises.

So in that case we would leave this in. Do a pretty good job of developing this impact list and then maybe map back to the - this long list of different kinds of processors and decide which ones could have the impact that we're concerned about. And in that case we would leave it in until we finish that. How about that for an approach?

Jacques does that address your concern about operational failures basically taking a bit different approach that your...

Jacques Latour: Hi. Jacques here. Those are - you know, if you lose, you lose a firewall, you lose a database, I think most TLDs have high availability infrastructure. So I don't think we need - we need to look at the impacts, assess them...

Mikey O'Connor: Yes.

Jacques Latour: ...and figure out what security impact somebody compromising your database. If they compromise the database because a router failed, I don't think we can - there's an infinite number of failures we can assess. But there's a limited number of security traps that we should focus on. But I think that's, you know, is cluster processor fail that's in the weeds. We don't even need to talk about stuff like that I think.

Mikey O'Connor: Yes. I think - I tend to agree with that. Rick, go ahead.

Rick Wilhelm: Yes. I wanted to - one of the things that I don't know if this came up before but there was a document that was published on this with the new gTLD registry transition process. Are folks familiar with that paper? There was - it was called an explanatory memorandum. I will paste - command C - all right - command V. Can't chew gum at the same time.

There was an explanatory memorandum put out by the new TLD program that described the gTLD registry transition process model. And it covered a fair number of these things and talked about how the new gTLD program was supposed to work. I think that might be interesting reading.

I personally have done a little bit of work with staff on that. And then subsequently it's the SSAC issued a set of comments on it. I also sat on the SSAC with a bunch of other folks and was part of the - this SAC 047. I pasted that URL into the chat window also. And so that might be interesting reading for folks to take a look at both of those just as far as the way that ICANN is proposing to deal with these things.

And the new gTLD program might help inform us with some of the security and stability things because taxonomy of problems are somewhat the same, so.

Mikey O'Connor: The reason your screen is blanking out is because I'm pasting those links that you and (Rocepa) put in into the background materials.

Rick Wilhelm: Yes. And Greg just put something into the chat window that yes, Patrick Jones is a resident expert on that stuff. He was the staff person that I believe led that effort and solicited and facilitated - solicited comments and facilitated discussion. I believe that Greg was part of that discussion team too. But I'm pretty sure. Is that right Greg?

Mikey O'Connor: I think I got this list from that document.

Rick Wilhelm: Okay.

Mikey O'Connor: I'm not sure about that. And that's part of the reason that it got into here is because I'm sure that I reviewed SSAC 047 and I think I also reviewed a registry fail over document. But I've run out of screen real estate to be able to check it on the fly.

Rick Wilhelm: Yes. Sure.

Mikey O'Connor: So maybe what we do for today is - goodness, what was that all about? Sorry. Got that. So I think then what we would do here is perhaps rather than giving it a complete thumbs up bright green, how about a nuanced pale green for its color like that. Not very nuanced. Pretty bright green. Not liking that a whole lot but I'm not going to spend any more time trying to figure it out.

We'll - why don't we - why don't we treat this one as possibly in scope but needs work. Just make note of that in our scope statement for now. Okay. Rick, is that an old hand or is that a new hand for a new thought? If it's an old one you can just take it down.

Rick Wilhelm: Old hand. Sorry.

Mikey O'Connor: Okay. Here's one that we can talk about in terms of scope. What would people think about sort of government intervention in terms of impact on the DNS? Now I have to go and space if this is - oops, it's up again. I assume that's a new hand now Rick. Go ahead.

Rick Wilhelm: New hand. So one of the things that's worth talking about in terms of government intervention and the DNS is the impact of legislation such as what's currently pending before the U.S. Congress, the Protect IP Act or whatever it's called, son of (quaka). And then the - and then it's related impact that they're talking about using DNS filtering as an example.

And then there was also a paper that was published by, you know, I guess what you might call some DNS luminaries, (Crocker), (Dixie) and some other folks that got published. I can work on digging that URL up.

That as an example of what it were - some folks are kind of speaking out that's saying that, Look, if we do this - if government's mandate - specifically U.S. Government mandate says DNS blocking, that causes some other, you know, sort of bad affects.

Mikey O'Connor: So I would interpret that to say that this one's in scope. Do that unless I hear shrieks of protest. Here's a dark green. Ah, there we go. Now that's a nice dark green. And that's going to help me remember which ones.

Are there any in here of the sub branches of this tree that are out of scope if people want to refine this or shall we take the whole thing as in scope? Take the whole thing unless somebody cries out in pain. We can always come back and change this.

We're actually quite a ways down our work plan doing this kind of work. So I'm feeling pretty comfortable in terms of taking a little time to do this. But if we get it a little bit wrong, I'm also fine coming back and fixing that. Okay. Go on to sort of physical threats.

Here maybe we've got misplaced stuff. That one up in there. Look at this one. This one - ooh, lots of (financial). Let's get the terrorism one out of here. That one seems a little bit misplaced. Pull this one up in here. This is a little bit purer.

What do people think about this pile now now that I've taken some of the political stuff out of it? I think again this was lifted from the registry fail over stuff that Patrick worked a lot on and some of the others of you helped with. Is this an in scope kind of thing? Let me phrase it another way. If I put it in scope, would anybody object? Now listen - cries of pain and anguish. Greg go ahead.

Greg Aaron: Physical issue. I think you have - this is one you have to put in context. And if we're talking about a root server to TLD operator, then yes; but physical or natural disaster on its own without any context doesn't - isn't perhaps helpful.

Mikey O'Connor: I think that's right. So let's say - like that. Does that capture the thought that you've got Greg?

Greg Aaron: I'd almost rather see a category of threat factors that affected (three servers), something like that. But yes, I mean that's okay.

Mikey O'Connor: Well let's say threat factors refinement that - how about that?

Greg Aaron: (That's okay).

Mikey O'Connor: So that one we'll give a green tick mark too. Move on. Got this one. (Fruition) of IP4. I can't remember where that one came from. I think - well, I guess it's from SAC 12. Greg is that a new hand or an old one? Talk about one or - does anybody have any thoughts about this one.

I'd have to go back and reread SAC 12 to see what the point was that they were making in this one. Maybe we leave this one as - for later discussion. And I can sort of take a first pass at some of these once we've got a bit of a feel of what the sense of the group is on this. Same with Fact 9.

Well this one's the alternate route scaling - I think the blocking - well I guess the reason I put those in there was because of the notion that the root would fragment. And I guess I would assume that this is in scope.

That a fragmented root would be a pretty dramatic problem for the DNS and I think it has to do with the paper of luminaries link that Rick pasted into the chat because I think the concerns that are being raised by that group if I - been a long time since I read that paper so I can't really remember.

But I think their concern was mostly about fragmenting of the root. And so I would assume that this would be something that we'd want to leave in our scope at least for now. So I'm going to do that again unless I hear howls of protest.

And then we had one left over that was - oh Olivier's got a comment. Let me - Olivier, you want to jump on the bridge and sort of make that point to the whole group?

Olivier Crepin-LeBlond: Thank you Mikey. This is Olivier for the transcript. It's just a general comment that we appear to be focusing primarily on the root and I just wanted to remind everyone we are dealing with the DNS security and stability.

So I don't think that we should just restrict ourselves to anything that might affect the root. It's really down to the actual - I believe and maybe others disagree with me but I believe that as far as DNS security and stability is concerned it also involves each one of the top level domains not only at root level but underneath that. Every zone out there. If a zone is going to be unstable, that's going to make the whole DNS unstable. Thank you.

Mikey O'Connor: Ah. Well that's a very tasty scope question. My interpretation of the charter, and I need to circle back to you charter writers like Greg and others, was that we would not go down to the individual second level domain zones but that we would stop at TLD. And so it would be root and first level DNS that was what we were throwing in on.

If we go to the second level, that's a pretty big - well, that's more than pretty big. That's a very big expansion of our scope. And I don't think that that's correct. (Yorg) is agreeing with me. Let me just see if I can drag up the charter real quick here.

From a TLD perspective is the phrase there. But then if we got to the - sorry to do this to your eyes as I scroll. Yes, here we go. Issues at the root and top-level domains. So I think that the charters Olivier were pointing us one level above second level. Is that - can we continue...

Olivier Crepin-LeBlond: This is...

Mikey O'Connor: ...to operate under that assumption or...

Olivier Crepin-LeBlond: This is Olivier. Again, yes, root fine. But top level also means the actual servers of the top-level domain provider. It doesn't just remain the actual root itself.

Mikey O'Connor: Ah. I - okay. I think the...

Olivier Crepin-LeBlond: So you see what I mean?

Mikey O'Connor: Yes.

Olivier Crepin-LeBlond: It's stability of the actual - the registry's equipment and so on is something that is involved in that. Whilst if we just remain at room level, then it would just be the root servers in which case some registries wouldn't have anything at root. We would just have their domain - their top-level domain at root level but it wouldn't be running a root server.

Mikey O'Connor: Right. I agree with that interpretation. What I heard you say was that we were going to take it down to the zones below the TLD.

Olivier Crepin-LeBlond: No. We said - sorry, we were not going to take it to each individual domain of course. That's ludicrous. That'd be...

Mikey O'Connor: Yes.

Olivier Crepin-LeBlond: ...(unintelligible) of potential...

((Crosstalk))

Mikey O'Connor: That's a lot of landscape for sure.

Olivier Crepin-LeBlond: Sorry about that. I might have not made my point clear. Thank you.

Mikey O'Connor: Yes. I think that there's pretty broad agreement to the notion that it's not just root infrastructure. It's also a TLD infrastructure. And so I think we're set there. Okay. So I'm going to - back to sharing my threats gizmo. Certainly getting a workout on Adobe Connect and I'm learning some things that if I were the kind of Adobe Connect I would change their user interface, but I'm not, so.

It takes me about six clicks to get back to the place that I was. Sharing my screen there. Okay. So given that, then where we're at right now is - this is just a question. In the notes from Singapore we had a threat that was called physical year 12. And I had no clue - oh my gosh. We're out of time.

Got so entranced. I'm sorry. I'm going to cut the call right off. (Yorg)'s departure reminded me. So damn. I'm really sorry about running over like this. We'll stop right here. We'll - is - let me do a quick feedback check. Is this kind of conversation useful? Should we keep doing this for a bit on the next call or shall we do something else? Give me just a thumbs up or a thumbs down or some indication that this is sort of the right approach.

Getting some thumbs up. So I'm not getting any thumbs downs. Okay. We'll carry on with this on the next call. My apologies for losing track of time. Thank you all very much. And we'll see you next week. That's it for me. Bye bye.

Cheryl Langdon-Orr: Thanks Mikey. Bye.

Mikey O'Connor: Yes. Sleep tight Cheryl.

Man: Thanks very much Mikey.

Mikey O'Connor: I'm sorry I had to wake you up this morning.

Cheryl Langdon-Orr: One of the times when I try and beg off. Never mind.

Mikey O'Connor: Yes.

((Crosstalk))

Cheryl Langdon-Orr: ...teach me for trying to apologize. I just won't apologize in future or anything. Of course you know that - don't...

END