

Transcript
DNS Security and Stability Analysis Working Group (DSSA WG)
10 May 2012 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 10 May 2012 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-20120510-en.mp3>

Presentation will be posted shortly on:

<http://gnso.icann.org/calendar/#may>

At Large Members

- . Cheryl Langdon-Orr (ALAC)
- . Andre Thompson (At-Large)
- . Julie Hammer (ALAC)

ccNSO Members

- . Jörg Schweiger, .de (co-chair)
- . Katrina Sasaki, .lv
- . Rick Koeller, .ca (CIRA)
- . Jacques Latour, .ca (CIRA)
- . Wim Degezelle, CENTR
- . Takayasu Matsuura, .jp

GNSO Members

- . Mikey O'Connor - (CBUC) (co-chair)
- . Greg Aaron (RySG)
- . George Asare-Sakyi - (NCSG)

SSAC members:

Jim Galvin (SSAC)
Warren Kumari (SSAC)

Expert:

Scott Algeier

ICANN Staff:

Julie Hedlund
Bart Boswinkel
Nathalie Peregrine

Apologies:
Olivier Crépin-Leblond (ALAC) (co-chair)
Mark Kusters (ARIN); (co-chair)
Don Blumenthal – (RySG)
Nishal Goburdhan (NRO)
Rafik Dammak – (NCSG)

Nathalie Peregrine: Thank you very much, (Tonya). Good morning, good afternoon, good evening. This is the DSSA call on the 10th of May, 2012. On the call today we have Mikey O'Connor, Warren Kumari, Jacques Latour, Cheryl Langdon-Orr, Andre Thompson, George Asare Sakyi, Jacques Latour - said already; I do apologize - Takayasu Matsuura, Julie Hammer, Katrina Sataki, Jörg Schweiger, Rick Koeller, (Unintelligible), Wim Degezelle, Greg Aaron and Jim Galvin.

From staff we have Bart Boswinkel, Julie Hedlund and myself, Nathalie Peregrine. We have apologies from Olivier Crépin-LeBlond, Mark Kusters, (Michelle Gabourdin), Don Blumenthal and Rafik Dammak.

So I would like to remind you all to please state your names before speaking for transcription purposes. Thank you very much and over to you.

Mikey O'Connor: Thanks, Nathalie; as always making everything work perfectly. Welcome all to the call. We'll take just a minute and run through the agenda and while I'm doing that if you have a change to your statement of interest you can raise your hand and we'll get that taken care of.

We're really going to do two chunks of brainstorming today. We're getting down to the point where, you know, we've got at least a first cut at a lot of this material and we've got a couple of portions of the report where we may be saying most of this stuff will have to wait until next phase.

But we've been at this a year and we may have some thoughts that we want to stick into this report both about immediate recommendations and also sort of taking a look at how we structure the next phase. The Ops team started this. We've got an idea that we kind of want to try out on you; get some reaction to that. And then we're going to spend most of our call on Monday - next Monday working on this again.

So those are the two big focus areas. I think we'll take sort of half the call on each. So if somebody could keep an eye on the clock and when we get to the 30-minute mark if I'm just waltzing on ahead without a break somebody nudge me and remind that I want to switch over at the halfway mark.

I've started a little mind map, which you can see on the screen. And up on top those legs - those four legs are basically the four legs of our charter. What are the immediate actual threats to the DNS? What are the current activities that are underway? What are the gaps in those? And what are possible additional mitigation activities?

And for the last three I think it's perfectly reasonable for us to say well hard answers to those three really have to wait until we're done with the next phase. But at the same time we've been looking at this pretty hard for a pretty long time and there may be some blindingly obvious things that we already know that we want to let people know about when they read this report. And that's really the purpose of this part of the conversation.

Let me show you a picture that - last time I mentioned that we needed to sort of draw a picture of something in the report and I've gone ahead and drawn a draft of that. This is that circle diagram that I talked about that said, you know, there's stuff that goes on in the core and there's stuff that goes on at the edge.

And there's connections in between the core and the edge. And we are but a part of the sorts of things that go on in that. And so I drew this picture based on the words that we went through in the last, you know, in last week's call.

And then I exploded that picture based on a conversation that we had on Monday with the ops group in which I put a little more context around this triangle. This is the go-fast versus go-deep picture. And where this started, just to remind people, is this picture. This is essentially a reworked version of the picture that we've been using out of the methodology.

And what we did is we took the five broad topics that we've come up with so far and we sort of arrayed them - this is - the putting them on the diagram is really my first try at this. This hasn't been reviewed by the ops team yet.

But the thought here is that as you get closer to the edge, which in this part of the triangle is at the bottom, that's where the rubber meets the road; that's where front line providers are meeting threats. And as you get closer and closer to the edge they're meeting those threats on a shorter and shorter timeframe.

So, you know, the most extreme of that would be, you know, somebody misconfigures something and somehow it brings down the root. That would be an immediate sort of problem that needs to get fixed right away. And this giant ponderous process that we go through probably isn't going to do them any good; they're going to have to react much faster to that than something like what we're doing can handle.

And at the other extreme is the policy management leadership sort of stuff, the very top, which is a very slow-moving, long-term, strategic kind of risk to the DNS. And so that's something to ponder.

Then what we have started to think about in the ops group is that what we could do is let's do one of these first in the next phase and refine the tools

that we've got. And then once we've got a refined set of tools that we could use more broadly recruit a much broader community to help do the last four.

So I just wanted to kind of splash that in front of you before we go back to this conversation about where we're at in the - especially these three topics. And at this point I'd just like to throw it open to brainstorming about any of these things that we might want to talk about in the report a bit.

This would have to be pretty brief, you know, more introducing topics than anything else. But if there's something that we can draw from the work we've done so far with reasonable underpinnings it would be a shame not to take advantage of that opportunity.

So there you go; there's an introduction. Now I'm going to be quiet. Oh and Nathalie has asked that those of you who are in as a guest in the Adobe room if you could identify who you are. If you're just listening in you could type your name in the chat and while you're doing that I'm going to go kill my email program so that it doesn't annoy me throughout the rest of the call.

Going once; going twice on guest. If you don't identify yourself we'll probably knock you off the Adobe room because it's not fair to the others to have an anonymous person - oh Scott's typing. Oh, Scott's typing about something else. Last chance for guest. Okay I think we're going to - if we can. Nathalie, do you know how to knock somebody out of the Adobe room?

Nathalie Peregrine: I'm not entirely sure. I was going to have a look now, Mikey.

Mikey O'Connor: Okay well if you could make a project out of that that would be great. Yeah, I'm with you, Warren, if I were that person that would surprise me and then - I suppose that we could start a private chat...

((Crosstalk))

Mikey O'Connor: And...

Man: I've started that.

Mikey O'Connor: Oh good, okay. All right so while we're sorting out who the guest - none of this is terribly secret; I just don't think it's fair to the rest of us to have an anonymous person on the call.

Any thoughts about any of those three topics, you know, current - we could just start with one if you want. You take a look at these threats and then. You know, one of the sources of ideas that I've got for this is the SSR framework that Patrick and others developed.

And, you know, there are all sorts of related organizations ranging from OARC and Scott's gang and so on that I think we can acknowledge. And I thought at least a reference to the SSR framework would be a good thing to put in this area because there is a lot of stuff going on; it's not as though we're just drifting along with no activity. And so I'll start with that.

But if there's something especially on people's minds that people want to - and I just type a few in that come to mind for me. You know, these are the sorts of things that I think we should acknowledge.

Cheryl Langdon-Orr: Mikey, Cheryl here.

Mikey O'Connor: Go ahead, Cheryl.

Cheryl Langdon-Orr: I was just thinking that would be the spot that we would also put in current activities from the ccTLD community as well.

Mikey O'Connor: Can you...

Cheryl Langdon-Orr: Well I would suggest we ask them to fill in the dotted lines. But clearly, you know, current activities to mitigate risk occur in the parts of root that they're in charge of as well so.

Mikey O'Connor: Oh I see what you're saying. Right. Some of you ccTLD folks...

Cheryl Langdon-Orr: Uncle Bart.

Mikey O'Connor: Yeah, any sources of lists that we could mine for that? I was sort of looking for Jörg but I guess he's not on the call today. So, Bart, you're stuck in the spotlight on this. Is there a document that we could at least point to that we could acknowledge in this part of the report? Bart's remarkably quiet. We'll put that on a to-do list.

Probably the same, you know, a lot of this shows up in the SSRT. And it would be probably good to summarize that. I think that the thing that I'm really interested in is maybe the next one. Are there, you know, this is actually a chance for people to throw out ideas that have been on their mind perhaps for quite some time about things that are missing in what we're doing right now.

If we - for example, I think that if we were to take a look at this one quite a number of the recommendations in the SSRT report fit in here. And I was planning to stick some of them in. Let me just see if I can quickly get to that. I started sticking some of this in. Yeah, see.

If you look at - this is a list of some of the recommendations from the SSRT report. By the way, there's a Webinar I think today about that which if you haven't heard about it let me know off-list and I'll send you the info. There's one going on right around now and then there's a later on that I'm going to attend in my afternoon; evening in Europe, early morning in Asia.

Jim Galvin: Mikey, I thought those - this is Jim Galvin, sorry. I thought those meetings were tomorrow; they're not today.

Mikey O'Connor: Oh are they? I thought they were today. Let me just check.

Jim Galvin: Well if they were today then I missed mine because I thought they were Friday the 11th.

Mikey O'Connor: Oh you're right.

((Crosstalk))

Mikey O'Connor: Yeah, you're right, there it is. Correct, correct, correct. Thanks, Jim.

Jim Galvin: Okay.

Mikey O'Connor: All the easier for people to get invited still. So anyway that's one of the thoughts that I had was that some of the SSRT recommendations we could at least acknowledge in this section. And so there, you know, it's - the purpose of this part of the call is to give me other ideas of places to mine for ideas that essentially relate to the five broad areas that we've identified, you know, already.

I think it's hard to go into a great deal of depth here but I think it's perfectly legitimate for us to acknowledge some of the stuff that's going on elsewhere. And as I say if there are things that are on our minds that come out of this this would be a good time.

I'm not being overwhelmed and I don't want to drag you through something that's uncomfortable so I won't belabor this. And maybe what I'll do is go to what I've already put in my notes and see what you think of those. Let me make this a little bigger - easier to read.

Some of - so here's where I've already started acknowledging the SSR framework that Patrick and crew produced. One of the themes that's been coming out recently is this notion - this next note which is that our charter says that we're supposed to come up with essentially a unified view of all the threats to the DNS and then in this next chunk a unified view of all - presumably all the efforts and activities to mitigate those threats.

And one of the things that I am tempted to point out in the report - and I kind of want to try this idea out on you - is this idea that a unified view may be impossible that if I'm a front line operator of a TLD I may be doing a bunch of things that are essentially either invisible to the rest of us or not relevant.

And I'm wondering if I'm on the right track with that or not. You know, this is essentially another scope kind of problem where, you know, in our go-deep phase do we really want to go out and ask everybody about everything that they're doing to mitigate all threats to the DNS? And if so any of us over the age of 60 might want to drop off this study group because it may take the rest of our lives to get that list done. At which point it would be pretty obsolete.

So I'm thinking that we might want to at least hint at the notion that scope explosion is a problem with this unified view that we've been chartered with. I mean, basically what we've been doing for a year is fighting various and sundry scope problems with this charter. And I think that this is another.

Cheryl Langdon-Orr: Mikey?

Mikey O'Connor: Go ahead, Cheryl.

Cheryl Langdon-Orr: Thanks. I wondered whether you (unintelligible) point where the - the fifth point in your column there that says coming up with several perspectives doesn't to some extent address how we can approach the identified problem of a unified view.

And the other thing is could we suggest that in fact what we need to do to meet the spirit of intention of the original charter is perhaps to have a coordinated and accessible view as opposed to the term unified and what can be drawn out of that because there's a certain amount of harmonization is indicated out of unified which, as one of the original co-chartering, you know, head space people, wasn't kind of the actual intent.

It was some or to actually have the accessibility to the risk data than it is to real risk data instead of these assumptions; the ability to have a hypothesis and test it with what we're missing. And I think to some extent you may have actually addressed the identified problem with a unified view in the following point. That's it for me for now.

Mikey O'Connor: That's really helpful, Cheryl, because the unified view scares me. And it's nice to have a way out of that puzzler. And it also hints at this notion of an ongoing thing that's got a - if I go back to this - it's sort of got a core and an edge where at the core - I mean, you know, there's a lot of stuff that could be made accessible in terms of tools, in terms of techniques at the core without having to perhaps document every single thing that happens at the edge.

The surface at the edge I think is awfully big. And I think that's the - one of the tensions that we've been fighting all along so that's good.

Let me show you the next chunk of stuff that I've already started to write. This is very notesy and this is pretty close to the same draft that you looked at last week so I haven't distributed it again because it's - it hasn't evolved enough to drag you all the way through it again.

But, you know, again you can see the SSRT report starting to show up. And again this perspectives thing is an emerging theme. And again the unified so let's just highlight Cheryl's words there. Wait no - why you did that - there we go. This is sort of the same theme. And again we've got that same notion; this several perspectives.

And I think we may want to introduce rather than come up with because there's no way we're going to do that between now and Prague. But that does take some of the pressure off us old people who don't have another decade to live that want to see the end of this project before we croak.

This is where the - the last section of this little brainstorming thing is is where I stuck in a bunch of the recommendations from the SSRT report. And I thought we would just acknowledge those and perhaps give it a thumbs up in general.

Because a lot of the struggle that we've got has to do with how undefined this stuff is. And it would I think be really helpful for some definition of a lot of these things. And I think we've done a fair amount of that definition ourselves because we had to. But I don't think it's our remit to answer these questions; we're simply part of the struggle. And so that was sort of where I was headed with that part of the report.

Recommendation 23 - interesting word glitch. I don't know what that's all about. I'm not being overwhelmed and I don't want to drag you through this anymore. Is there anything else that people want to talk about one last chance on this trio of topics? I'm going to go ahead and draft some stuff and you'll have a chance to edit that draft.

But I was just wanting to get a sense as to whether I'd missed anything big in the direction I was heading. So this is your last chance on that one. Okay let's do the next phase.

And let me go back to that picture that we in the ops group have started to draw. What's coming into my mind at least is the idea that what we should perhaps try to focus on is to develop a tool or two that lots of people could then participate in using - to generate some of these results.

I hesitate to say it in the context of Cheryl but, you know, it may be that it's some sort of polling or survey gizmo based on that - that worksheet that we built. Or it may just be a refined version of that worksheet.

And so the thought that we've been playing around with in the ops team is that we really ought to do one ourselves - the DSSA only. Dig in, make sure the tool works, make sure we understand how to do the analysis based on that. And then once we've got the first turn of the crank done at a minimum break into sub groups across the four remaining, you know, these four - see if I can figure out a way to highlight those - doesn't really do it but there you go.

And essentially run out to a broader community of interest with the now newly refined tool. Essentially as a beta test of tools that then the goal would be partly to finish our report but would also partly be to deliver a tool set to the community that they could use to do their own risk assessments in their own context.

And if that seems like a reasonable approach to you the ops group is right in the middle of this conversation. But I wanted to take a minute and just get your ideas on this as well. And so these are just the standard project management topics.

When you all, who've lived through this for a year so far, look into the future are there some things that we should do well? Are there some things that we should avoid? Are there some things that we should do differently? You know, at least from my perspective I'm very concerned right now about burning ourselves out.

You know, we've been at this quite a while and I'm really worried that we're, you know, we're steadily dwindling in number. And at least for me there's, you know, the sense of sort of this finish line at Prague and then I'm planning to sort of throw down my tools and say I'm not going to carry quite so much of the load going forward because I'm getting pretty burned out on this myself.

Cheryl Langdon-Orr: Mikey, Cheryl here.

Mikey O'Connor: Yeah, go ahead, Cheryl.

Cheryl Langdon-Orr: To some extent what you've just said about the burnout, etcetera, leads into the question I wanted to raise and that was with the do-it ourselves, do one ourselves issue I was wondering about the timing on that. And I'm certainly supportive of breaking up into the workgroup - the workgroup into some sub sections and dealing with the real (unintelligible) acquisition stuff that follows on those other four areas.

The timing on that would be post-Prague, which in itself would make a difference to how the resources are currently being exhausted or otherwise. But I would note that, you know, you've got 17 people on this call and I wouldn't call that a dwindle. We've actually been incredibly stable on I think very good numbers for a workgroup of this (unintelligible). It is dyamic...

Mikey O'Connor: Yes. Yeah, yeah.

((Crosstalk))

Cheryl Langdon-Orr: I'm not - as a manager of volunteers for many years I am less concerned about burnout generally than you are but I am keen to re-distribute tasks in the next phase. Does that make sense to you?

Mikey O'Connor: Yeah, it sure does. I think that one of the things that everybody's quite conscious of certainly in the ops group but I think the rest of you too is that this is too much gated through Mikey at this point and that has to stop because I'm becoming the bottleneck right now. And so we have to figure out a way that this can be done that doesn't have me as the bottleneck in it going forward. And I'm really interested in ideas on how to do that.

I didn't really see this coming until a couple of months ago and then said well okay I'm going to carry it through Prague as the bottleneck because it's hard at this stage to unwind that. But I really, really, really don't want to pull quite so much of the weight going forward.

Cheryl Langdon-Orr: Okay Cheryl again for the record. First, Warren is nudging you at the 30-minute mark. But secondly I think the pre and post-Prague activity plan sort of meets that need, Mikey, part of why you're good at what you do of course is because you're good at what you do. And if we disagreed with you you'd hear about it. And in many cases I think you're far less of a bottleneck than you think you are.

Mikey O'Connor: Well I...

((Crosstalk))

Cheryl Langdon-Orr: You're one hell of a foundation-builder but as we...

Mikey O'Connor: Yeah.

((Crosstalk))

Mikey O'Connor: It's more the resource problem, you know.

Cheryl Langdon-Orr: Yeah, as you mentioned...

Mikey O'Connor: Sorry to interrupt.

Cheryl Langdon-Orr: ...the next phase...

Mikey O'Connor: Yeah.

Cheryl Langdon-Orr: ...that by necessity the design changes resourcing.

Mikey O'Connor: Yeah. And I think...

Cheryl Langdon-Orr: And for example to go deep on - to do a run through on the tool would actually take not a bunch of one-hour calls but I would suggest probably a serious block of face to face time where you sort of, you know, sit down and do the hypothetical as such. And that would be, you know, now that no Fridays committed to Board meetings we might need to re-jig, you know, a face to face forum at some opportunity with obviously remote participation.

Anyway I'm going to stop there because there's a million ways of skinning that cat but I think now is the time - we've got the cat to skin at this point.

Mikey O'Connor: Yeah, I think it's - it's really important to - yeah - redistribute tasks but also restructure the work. Now let's brainstorm about what that could look like for a minute. What are some - and that would go up in here I would think - really up here.

What are some things that we could do that would make this more - and by the way, we have passed through the 30-minute mark but we've also changed to the second half of the agenda so I'm fine with that. Oh my God I just now looked at the chat. Hang on a minute. I have to catch up.

Yeah, oh scope, yeah, let's get scope in here. Just picked up Rick's comment. And then Cheryl is right on the beam; this is exactly what we were thinking about on the ops call was that we would do one as an example, as a sample to test this. So what we were - one of the things that came up in the ops call was that our charter is to make sure that those four charter questions get done.

You know, it's at least the sense of the ops crew that we have to at least come up with a credible answer to the question what are the current risks to the DNS. What are the current mitigation activities, etcetera.

Jacques Latour: So Jacques here.

Mikey O'Connor: Go ahead, Jacques.

Jacques Latour: If I recall all of this started about two years ago when Rod made the statement, right?

Mikey O'Connor: Right.

Jacques Latour: And if you look at the story for the charter is there are threats that are happening over the Internet and we've documented on the DNS we've documented a few of those, right?

Mikey O'Connor: Right.

Jacques Latour: The activities to mitigate these threats internally, individually each organization I think has good mitigation techniques to handle the threats. And the third bullet is the gaps and the current security response to DNS issue.

So I think the big thing back then was ICANN wanted to create a global cert for handling DNS. And perhaps one of the - it's true, there is a need for that. If we have a multistakeholder denial of service attack or a major threat to the DNS today there is no global method for all of us to join - to do incident resolution.

There's isolated fragments of systems or process in place like DNS-OARC which is based on the trusted model but it's not a globally accessible system by all that operates the DNS. And my gut feeling is that the idea behind all of this is there are threats; we can mitigate them but there's no global security (unintelligible) requirement and we should a create DNS cert within ICANN or something like that.

Does that - that's one way of looking at it.

Mikey O'Connor: I think that this is - hang on - I can see Greg type - Greg, you want to just jump in on the call? I have a feeling I know where you're headed. It's going to be hard to type that all out. Yeah. I think that - I think that we could draw a picture - this is part of the reason I drew the picture this way is that I think there are some things that can be shared in the middle. But I'm not sure that ICANN is the right organization to run it.

Cheryl Langdon-Orr: Hell yeah.

Mikey O'Connor: Yeah.

Cheryl Langdon-Orr: Certainly not.

Mikey O'Connor: You're getting plenty of yay verily in the. And so I think that the - you know...

Jacques Latour: It's Jacques here.

((Crosstalk))

Mikey O'Connor: ...back to what you were saying I think that what we could say that would tip toe around the words ICANN operated cert, which is a red flag, is instead to say that, you know, we could look into ways for the community to join together.

Jacques Latour: Yeah, Jacques here again. Yeah, I'm not - I'm against the ICANN DNS cert.

Mikey O'Connor: Yeah.

Jacques Latour: But I think the purpose of this charter was - might have been to justify that or somehow...

Cheryl Langdon-Orr: No it wasn't.

Jacques Latour: ...or identify the need for a central place for all DNS operators to be working together. I'm just thinking - I'm trying to - because I don't think we need to go to look at all the threats in great depth. I don't think we need to go to a great depth in like mitigating all the threats. We've done some of that.

It's how do we - the third bullet is how do we respond to these issue individually and collectively?

Mikey O'Connor: Right and so I, you know, I think that part of what you are saying is consistent with this section - the current activities. And I think the way to summarize that is that there are a lot. And for the most part they're effective although we don't have much data to support that conclusion.

But that there - you know, there's this - you know, and I guess the key to this phrase is - I'm not sure there's no global way. Or maybe...

((Crosstalk))

Jacques Latour: There is...

((Crosstalk))

Mikey O'Connor: It's - yeah, it's almost...

Jacques Latour: Well put it this way: If something really bad happens right now there is no group or there is no way...

((Crosstalk))

Jacques Latour: ...there is no way to get all the ccTLDs on the planet on the same phone call with the gTLD operator and everybody.

Mikey O'Connor: Right.

Cheryl Langdon-Orr: And that can be a recommendation and fix. But to have the playing field for that to happen we need to have shared knowledge and agreement on data sets and the actual risks that we're dealing with. So - this is Cheryl for the transcript record.

Part of the problem was in the dreaded statements from the CEO was that in raw number terms you can stand up and say there were X threats to the DNS happening daily. But there was no indication on what affect mitigation had in that number. And in fact what the resiliency and stability effects of any of those were. It's a little bit like having 1000 flies biting you versus a tiger.

And - yeah, so the need was for real data sets and actual metrics and analysis to be done. It's a vastly different thing if we come out with an end point here that says we are in fact under current constant, in inverted commas, attack but they're all being handled really well and we don't need to worry about them versus there's a great bleeding hold over in the corner there and no one's actually driven a stake through it yet but we think they could do and that needs to be dealt with.

And it's driving the stake through the great bleeding hole while causing the great bleeding hole in the first place that we need to be able to set up the likelihood and responses for and that's where the missed stuff, I think, is such an excellent tool. But rest assured, Jacques, there was no way that the DSSA's charter was in any way to support the creation of a cert. If anything it would be to do the opposite. Thanks.

Mikey O'Connor: Yeah, I would agree with Cheryl. In terms of history - oh Warren came in with an OARC point. How broad is the community that's in OARC, Warren? Is it broad enough to be actually representative or could it be that that community isn't terribly interested but that they don't include folks like Jacques?

Jacques Latour: Well nobody - this is Jacques - nobody trusts me, right, so - actually I'm part of - we're part - serious part of OARC.

Mikey O'Connor: Oh okay. So you were in those discussions maybe too?

Jacques Latour: Yes.

Mikey O'Connor: Oh Warren's got no audio; that's too bad. I'm liking this conversation. We're back at the first part but actually I'm pretty intrigued with where we're going here. So I think I'll throw the next phase discussion over the side of the boat and we'll stay on this for the rest of the call because in a way one way we could write this report is to say look, we have done a bunch of stuff on this first charter item, threats to the DNS.

Look at what we've done. We've struggled with scope of what's the DNS in and out; we've struggled with confidential information and how to handle it; we've struggled with methodology and we've come up with some cool tools with NIST. Then we've come up with five broad threat areas. Way to go us.

There are a lot of things going on. Look at this list and, you know, we could go built that list out of all those sources. But what it really comes down to it seems to me in a way is this dilemma which is I think that the notion that Jacques kicked us off with was that there's no global way to very quickly collaborate on an emerging threat.

And I think a lot of people would say yes that's true. The problem is where is that forum to be convened and who's supposed to have responsibility for it. And that's where the conversation goes off the rails.

Warren Kumari: Yeah, this is Warren. I mean, we've had multiple, multiple discussions over the years about (unintelligible) so especially during the whole ICANN cert

thing there was much gnashing of teeth and oh my God not ICANN doing this, etcetera.

And DNS OARC seemed to be sort of the generally accepted - generally accepted by the community option to (unintelligible) that people liked first or, you know, any of the other huge collection of random cert people or yet another group to be spun off to do this.

But, you know, there are a number of sort of secret mailing lists where stuff like this gets discussed especially during the whole anonymous event or lack thereof; there were a number of those (spun off). And a bunch of discussion on the do we need some sort of things like this.

And what a lot of people kept coming back to is folks who actually care about this have methods and solutions in place. You know, if you care about the stability of the DNS and what's going on currently and incident response type stuff OARC seems to be the place where people discuss this.

Yes there could be a much larger organization (spun up) with, you know, everybody able to participate. But who's actually going to spend the money, time, effort to build this? Who's going to provide all the infrastructure that's needed? Who's going to be the gatekeeper that let's the good guys in and keeps the bad guys out because unless it's sort of a non adversarial threat thing you don't really want the bad folks participating in your response.

So this is going to have to be another sort of ops trust type community I think, in my opinion. And there are secret ones like that that already exist. Of course nobody can speak their names, etcetera. But, you know, there are sort of solutions here. And I think I'm standing on a soap box and having a long rant so I'll shut up now.

Mikey O'Connor: I like people who stand on soap boxes and rant because that takes some of the stand-on-soap-box-and-rant pressure off of me so I like that. I think that

where this conversation is starting to head is that place where we sort of step back from the trees and look at the forest for a minute.

And I think that there's a kind of emerging parallel discussion. I resonate a lot with what Warren just said that when you're looking for a place to deal with an immediate front line threat that - and maybe this picture is helpful; maybe it's not. Let me go back to this picture.

Is it safe to say that down in this lower right corner, you know, here's a threat; it's happening right now - we need to respond within minutes - that that kind of coordination is pretty good today. Perhaps good enough and perhaps making it more visible to the world is counterproductive rather than productive.

While at the same time, if you go into the long term view, Cheryl's point comes to the floor, which is on this side which says that while there's reasonably good coverage of immediate threat mitigation there's an opportunity to do things out in the public where it doesn't really matter whether bad guys participate or not to develop tools and techniques and so on to help DNS providers do their risk - their immediate risk mitigation better.

Is that way to reconcile those two points?

Jacques Latour: Yeah, Jacques here.

Mikey O'Connor: Go ahead, Jacques.

Jacques Latour: Yeah, no makes sense.

((Crosstalk))

Jacques Latour: Get the picture now.

((Crosstalk))

Rick Koeller: Hang on. Rick speaking. And I think that's probably a better focus for Phase 2 scope than digging down and trying to analyze the deep pool of risks that have been identified.

Mikey O'Connor: Well that's part of the reason why we chose this one first is because this one sits in two places that we can help more than we - you know, this lower corner has a lot of disadvantages. It's very big; it's very secret; it should be secret. It seems to be reasonably well handled, etcetera, etcetera.

But this one sits on the tools, models, support direction end of the spectrum and seems like it's better suited to an organization like us to handle. So that sounds like this diagram is not too bad. And it also sounds like we've picked the right direction.

At the same time what we might want to do - oops - is write some of the stuff that we will now memorize as Warren's rant - into the conclusions of this phase report. Because in a way our charter was in response to Rob's rant back - you know, so there's a rant that starts this project and in a way there's a rant that ends it. There's the Beckstrom rant - oh it's a dangerous place and there are giant holes and so on and so forth.

And I think Warren's rant, in a way, puts a period on that sentence. It says no, you know, actually it's not as bad as you think; you just don't know about what's going on. And yet at the same time the whole community says yeah but we could always do better. And, yeah, we would benefit a lot from shared tools, shared data sets, shared knowledge, etcetera, etcetera.

Is that sort of a way to wrap up our conclusion in - yeah, I know, we're right on the time boundary. But I just want to get a sense is anybody just wildly upset by that sort of summary that says if you - you know, because in a way

then what we could do is we could come back to the community and say, you know, we've struggled and in a sense we're done.

We see lots of stuff to do and we're willing to do it. But in terms of the thing that triggered the DSSA, which was the Beckstrom conversation to the ccNSO in Brussels, we actually have an answer. Because I think that - up until now I hadn't thought that we could say that but we might be able to say that. It's probably one to - now that it's nine o'clock my time...

((Crosstalk))

Mikey O'Connor: ...it's time to stop.

Cheryl Langdon-Orr: That one's sticking in my craw just a little bit but anyway.

Mikey O'Connor: Yeah, well I think that's one to pick up again on the next call for sure. And, you know, it's partly a burned out guy speaking and kind of looking for an escape hatch. But at the same time I think we could hint at it in the report. And act on that in our next phase by saying, you know, where we're going to devote our attention is on the left side of this diagram and focus on models, tools, support, etcetera.

Yeah and Jim is correct...

((Crosstalk))

Mikey O'Connor: ...is saying - yeah, yeah, yeah, that's absolutely true. Okay I think we need to wrap up now but I think this was very helpful certainly for me and for the ops crew as we try to figure out where we're going. Nathalie, can you chop off the recording and we'll call it a day. Thanks everybody.

Nathalie Peregrine: Sure. (Tanya) please...

END