

**DSSA WG
TRANSCRIPTION
Thursday 26 April 2012 at 1300 UTC**

Note: The following is the output of transcribing from an audio recording of the DSSA WG meeting on Tuesday 26 April 2012 at 1300 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-20120426-en.mp3>

On page:<http://gnso.icann.org/calendar#apr>
(transcripts and recordings are found on the calendar page)

Attendees on the call:

At Large Members

- . Cheryl Langdon-Orr (ALAC)
- . Olivier Crépin-Leblond (ALAC) (co-chair)
- . Andre Thompson (At-Large)
- . Julie Hammer (ALAC)

ccNSO Members

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

NRO Members

- . Arturo Servin (LACNIC)

GNSO Members

- . Mikey O'Connor - (CBUC) (co-chair)
- . Rosella Mattioli (NCSG)
- . George Asare-Sakyi - (NCSG)
- . Rafik Dammak – (NCSG)

SSAC Members

- . Warren Kumari (SSAC)

ICANN Staff:
Julie Hedlund
Bart Boswinkel
Nathalie Peregrine

Apologies:
Jim Galvin (SSAC)
Mark Kusters (ARIN); (co-chair)
Don Blumenthal – (RySG)
Jörg Schweiger, .de (co-chair)

Coordinator: We're now recording.

Nathalie Peregrine: Thank you very much, (Ricardo). Good morning, good afternoon, good evening. This the DSSA call on the 26th of April, 2012. On the call today we have Mikey O'Connor, Cheryl Langdon-Orr, Olivier Crépin-LeBlond, Rafik Dammak, Warren Kumari, Andre Thompson, Arturo Servin, Rosella Mattioli, Julie Hammer, Wim de Gazelle, Takayasu Matsuura, Jacques Latour and Rick Koeller.

From staff we have Julie Hedlund and myself, Nathalie Peregrine. I only have apologies from Jörg Schweiger, Mark Kusters, Jim Galvin and Don Blumenthal. Bart Boswinkel has just joined the AC room.

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. And welcome all to the call today. We'll take our moment to check in on statements of interest see if any of those have changed.

All right, I apologize for how teeny, tiny the type is on the screen. This first agenda item is the one where we're going to try and sort of normalize these threat scenarios. And in order to get the whole thing on the screen I have to

make it awfully small. Is there anybody who simply can not function at this level of tininess?

Okay well let's see how this goes. If it drives you all crazy I'll try and figure something out. But I think it's helpful to be able to see all the columns at this. This is the summary spreadsheet of the threat scenarios. And really I think today what would be good is to go through each one and sort of see if we can iron out the wild difference in score in the conversation.

Just spend a couple three minutes one each scenario and just see if, you know, it could well be that there are these kinds of differences. But just, you know, since different people were doing these and they had different approaches and this is a first time through with a new tool it seemed like a good idea to just go through and check.

I think that probably it's too bad that Jörg isn't on the call today because - I'm going to scroll down - I think the one that sort of sticks out is in fact the one that Jörg did because it's so much smaller than most of the other ones. And I think that the main reason for that is that he skipped a column. See what column that is. Skipped any predisposing conditions that would have a negative impact on the thing and so as a result there's no value in there.

And so if I just arbitrarily put five in that value, add it to my scorekeeping - that's interesting. You know, this is homework before your very eyes. Why is J45 not getting into my equation? No. J45 to my equation. There. Now we get them up, you know, that's the sensitivity of this model.

I'm sort of doing this on your screen to show you I think what we're about at this point is to - oh except none of these have scores. Oh that's because this is not a scored column. Never mind. So I can't see why Jörg's score is different. But I think that's what we need to puzzle through today so that's what we're about. Sorry to stumble around.

I did some clumping so this first group of three is sort of the impact of the nation states tinkering with the Internet. But in all three cases these are sort of combined scenarios where the result of the scenario is not just one thing but several things working together.

So two of them came from Rosella and one of them came from me but really came from Scott Algiers's group that did the work for the National Information Protection Plan. And what they're describing is a sort of policy governance knowledge failure and it's very long - very long thing.

And here again we've got another interesting sort of normalizing issue where the reason that this is low is because of the choices of capability, intent and targeting by Rosella. The - and, you know, then some of these other columns.

So I'm not sure that the normalizing is as dire a problem as we may think. But I do think the poor old DDoS didn't get quite the number of points it needs. And - oh there's the one I missed. Just typed the wrong one so if I make that 5, that 2, yes.

So I think that the column that - yes - that Jörg missed was predisposing conditions that negatively affect things. And if I just put a sort of moderate value in there that sort of brings it up into at least the right order of magnitude.

Now another dimension of this conversation is perhaps the DDoS attacks are in fact fairly well handled right now. Better not take that out before I - yes, what I did. And that, you know, we could conclude that maybe DDoS attacks isn't nearly as much of a problem as we thought.

So there's a ramble. And now that I've rambled enough I finally got a bite out of Jacques so go ahead, Jacques.

Jacques Latour: Hi, Jacques for the record. So I agree with the number that there the risk factor was fairly low because, you know, all the TLDs have implemented good infrastructure to be resilient against DDoS. The control of the DDoS is possible but the impact would be fairly low because we've put in all - any (unintelligible) infrastructure to be resilient against that so.

Mikey O'Connor: Yes, and I think that that then - none of these numbers should be taken terribly seriously because, you know, this model is so touchy. Each column essentially adds or subtracts and order of magnitude. And so the fact that the numbers get very large and vary quite a lot I don't think is that big a deal.

And I think that one of the ways we could treat this is simply, as you say, Jacques, to say look, you know, there is good infrastructure in place. DDoS is something that's been known for quite some time. There seems to be pretty good response to that threat; the response is pretty diverse across the DNS, you know, the zone providing community.

And the fact that the number is quite a bit smaller doesn't indicate much of anything except that, you know, we tend to think that that's a threat that's not as worrisome as some of the other ones that we're looking at.

So with that what are people's reactions to this? Let's go from top to bottom just so we can kind of keep things straight. One of the ways we could do this as a group is we could give the owner of this - of each threat scenario a budget for each of the numbers.

So, you know, we could say to Rosella well your first try was fine but we disagree with you on that. And we could essentially go very quickly through these and just do a sort of a poll. I'm pretty anxious to try out my polling screen because I think it will make you all fall off your perches. Because I've got a version of the Adobe Connect where there are nine polls on one screen which I know will send Cheryl right around the bend. This is actually a joke back to the vertical integration working group.

So we could do that. We could have a conversation about each one. You know, at this point having built this spreadsheet I'm sort of open to all sorts of ideas as sort of how to proceed from here. Any thoughts if you were in my shoes trying to run this call what a good way to do this would be?

Yes, see, this is kind of a puzzler. And, you know, as I thought about this another way to approach this would be to publish these as example scenarios in our report. And preface this section of the report, which will be a very substantial part of the report, because when you turn all this information into text, you know, each scenario is going to wind up being a few pages long.

So the 9 or 10 scenarios that we have is going to wind up being 20-30 pages of report when we expand it out. And one of the ways we could approach that section of the report is to say look, these are example scenarios that we've developed as a group. And you, the readers of the report, should read this with a skeptical eye and we really want to hear from you about two things.

We want to hear from you if you think any or all of these scenarios are stupid and crazy and should be excluded. And then give us reasons why. And we also want to hear from the readers about scenarios that we just totally missed that they think we should add to our lists. And essentially leave it at that.

And maybe not even score them because the scoring at this stage, given that we don't have much in the way of data to underpin these scores, the scores are fairly arbitrary. And that the really useful thing about this exercise is identifying the scenarios and the vulnerabilities, controls, etcetera, that are related.

So again, you know, I'm really pleased with these; I like them a lot. And I'd sort of like to get a sense of the group if we go back to our charter our charter says actual vulnerabilities to the root. And I think that at this stage we have developed some scenarios that are real but we haven't analyzed them yet.

And we're going back to the community and saying here's how we plan to do it, here's how we plan to break the information up. These are our preliminary scenarios that we're thinking we'll take a look at. And what do you think?

If that was the case then we wouldn't have to fool around with normalizing scores at all because, you know, I think at that point we probably wouldn't score them in the report. We'd keep this because this is our destination and we certainly can use this framework.

But we don't need to get too terribly wrapped up in getting these scores absolutely right this time around. If people are comfortable with that approach then I think the other thing that we might want to do is talk a little bit about whether some of these could be combined.

Because, for example, we got, you know, we have these three that are fairly closely related; they're scenarios that involve nation state either blocking or alternate roots. These two are both from ISOC scenarios of the future Internet and are basically half of a two-dimensional matrix where, you know, the ISOC is concerned about essentially fragmenting the Net into walls gardens of one sorts of another.

And then three - oop, no I don't want to do that. Why did I get that? Oh. And then these three which are more, in my mind, in the sort of technical arena. And I think all three of those could stand on their own. And so what we could do is collapse these a bit.

And then for those of you who are saying but wait, where are my other ones the other ones are the non adversarial scenarios and they're on a separate tab because the columns are different and thus the scores don't correspond because there's at least one and maybe two fewer orders of magnitude in the analysis. So again be not concerned about the fact that the scores are quite different from these two pages.

And I put these two together because they were both sort of outage ones. Rosella's was a bit more improbable. She gave it a likelihood of zero which takes the overall score down a bit. And then, you know, I separated Jacques's because I thought that was quite a different kind of thing.

But, you know, it seemed to me that we could combine these, for example, tentatively anyway. And if we did that - if we combined those two plus, you know, I'm quite cheerful about the idea of combining my two and maybe taking these from three to two or maybe even three to one then we'd wind up with something on the order of six or seven scenarios to roll forward into the next phase which seems a good thing.

I am a believer in sort of the magic number seven. If we get too many things going it starts to get confusing I think. But before I did that I wanted to check with you again and see if that made sense to you as well. If I'm just cavalierly combining something that you don't think should be combined for sure - oh, Cheryl, you've got your hand up. You've had it up forever. I'm sorry, are you on the gizmo that won't raise - anyway go ahead, Cheryl.

Cheryl Langdon-Orr: Okay thanks. Can you hear me or not?

Mikey O'Connor: Yes, I can hear you fine.

Cheryl Langdon-Orr: Oh great, okay fine. Just rolling back a little bit I'm happy with the clustering as-is. And I too like seven because it's a perfect number for a wolf pack which is another conversation altogether.

But the - so the clustering, yes, I'm happy enough with - in terms of the likelihood score, the total score, yes, I'm less committed to having that being (unintelligible) published. Because I think there's an awful lot of thinking needs to go into that overall risk business. And to be honest we might end up

making it some sort of bizarre color coding rather than raw numbers which really are totally fudge factors at the moment as far as I can tell.

With your question as to what we should ask our report readers I wouldn't be asking them what they think of these examples as much as I would of your part two which would be what other things do they think should go into our example set.

Because I don't really care if they think they're easy crazy good or indifferent, they are what they are. But I would want to know from the wider audience have we totally missed a whole yard.

Mikey O'Connor: Yes, I get that...

((Crosstalk))

Mikey O'Connor: Yes, I think that's right. I think the reason that we might want to ask them about egregious errors is - I agree, less of an issue. Because we can weed that out ourselves I think. So I don't think that is...

Cheryl Langdon-Orr: You're being far too kind.

Mikey O'Connor: Yes, I really do have great confidence in this group for getting rid of silly stuff. I introduce silly stuff every time and the group straightens me out nicely. I think egg picture over bird pool picture for the cover of the report (unintelligible).

Rosella.

Rosella Mattioli: Hi, Rosella for the record. I don't know if - can you hear me?

Mikey O'Connor: Yes.

Cheryl Langdon-Orr: Yes.

Rosella Mattioli: Good. Well actually I was thinking about (unintelligible) the number of scenarios. Why don't we apply a modular approach like nation state scenario and then all the different possibilities regarding the scenario. And then we have like a matrix. And then we do the same for each high level scenario.

I was thinking just like in order to have like high level scenarios for each kind of (unintelligible) that we have here and also to have (unintelligible) more number just less than our seven as you were saying.

Mikey O'Connor: Oh I see - let me play that back because my phone was kind of soft and I was having a hard time hearing you. So essentially high level scenarios and then scenarios - sub scenarios under the high level ones? Is that what you were thinking?

Rosella Mattioli: Not exactly sub scenarios but then - yes, I was thinking like okay we have a nation state scenario and then we have all the different typology of threats and (unintelligible) listed here, listed as like all the possibilities that you can have within the scenario. So we have like nation states, DDoS, vulnerability like a major topic, and then listed all the different things that we have put in every single scenario. So just - that's an idea because we have to do this before Prague isn't it?

Mikey O'Connor: Yes, we're shooting for a report by Prague. And I'm confident that we will have one. I am sorry to admit that I'm not quite - I'm still not quite following your proposal. So I think try it all the way from the beginning again and let me see if I can understand it.

Rosella Mattioli: Okay. So we were talking about the fact that we want to generalize in like a major scenarios to the level - or to the number of seven the scenarios that we want to have for the final - for the presentation in Prague from what I understand.

So I was thinking that maybe we could like - regarding the nation state scenario instead of having like merging all together and like (unintelligible) some of the opinions that people put in them we could like have a nation state high level scenario and then listed all the different possibilities within the threat scenarios like in a matrix.

So it was just like a way to generalize the (unintelligible) of - all the work that all the people did in their single scenario. It was just one idea.

Mikey O'Connor: So let me try something here. Oh this is not going to work. Never mind. So what if we highlighted the fact that we have two scenarios that focus on nation states as the threat source. And so then what we could do is we could combine on nation states the threat source being nation states and then also combine all of the things that people wrote; is that basically what you're saying?

Rosella Mattioli: Yes.

Mikey O'Connor: Oh okay, yes, I think that's a great idea. So that when we do the combining - and this gets me back to a point that I was planning to make that I forgot which is that this number four items, you know, is purely a Mikey construction. It could be that our list is longer than that. And by doing the combining that way we give ourselves the opportunity to make longer lists that we can then go talk about in the next phase.

Is that also consistent with what you were thinking, Rosella?

Rosella Mattioli: Yes, absolutely.

Mikey O'Connor: Yes, okay. I get it. Thank you for your patience on that one. I have a pretty good feel for where I need to take this matrix for next week. Let me go ahead and do that and bring that back to you all for a review.

And I'm glad that people are okay sort of stepping back from the scoring because I think the scoring at this stage might be premature and might distract us a bit. We've certainly got a mechanism to do it but I think that it's helpful to step back from that a notch.

Now let me preview one other idea that I've got which is that in the next phase - in this part of the project of the working group we've been single threading our work mostly because we've been building our airplane while we're flying it and we need to keep ourselves together to make sure that we're in agreement.

But my idea was that in the next phase, in the more detailed phase, that we could break into not the super duper confidential information type sub teams but just sub teams that could work independently of each other on evaluating these scenarios so that we could begin to do some multi-threading here.

And I'm curious about your reaction to that idea. I think it would - one of the things I'm really concerned about is the dependency of this group on me as a sort of single point of failure. And I would really like to spread out the work a bit in the next phase so that we're less vulnerable to Mikey's screw ups. And I'm hoping that that's okay with the rest of you.

Now what that would probably imply is that we'd be meeting twice a week each of us as individuals because we'd meet in a sub team and then we'd also meet in the larger group to sort of share ideas and compare notes. And I'm curious if people are comfortable and willing to devote that much time to the effort.

So that whole package I'd like to put on the table and just see if anybody has any concerns or questions about that before we move on? Okay to everybody? Good deal.

Speaking of sub teams - oh and I've drifted away from the chat. Sorry, Arturo, I'm glad you sorted it out. This is - I should probably synchronize the version numbers so that this is the summary spreadsheet rather than the actual worksheet but that's a good point, I'll do that on the next round so that people know that the current version of everything is the version number. If I can. I have to think about that a bit. It may be less feasible than I thought as I think about it. Anyway, thanks for the point.

Okay onto the next thing which is - it's all about sand mining. I don't suppose you're interested in that. Let's see if I've got a - no. Hold on just a minute. There it is. This is the latest version of the confidentiality guidelines or the joint sub team stuff.

And I sent out a note with this draft that sort of summarized the big changes. And I just want to step through those again very quickly here on the call and see if we can get to sort of a preliminary consensus on this today; if we can't that's fine but if we can that would be good because that would get us nicely on track to get this into the report for Prague. But again no pressure. If there's still an issue we need to keep at it until we get that right.

Scrolling quickly through this I think the first big change is the work that I stole from Julie Hammer. Julie raised this on the last call and then she and I had a conversation by email that fleshed this idea out and I then promptly stole it and crammed it into this draft that said well as you can read that it would be good maybe to have a tracking mechanism to record sort of the nature and status of these bits of confidential information.

So I just inserted it. And I wanted to make sure that that was okay with people. So there's the real meat of it which is a description of the confidentiality information - or the confidential information.

The one that caught me and needed clarification from Julie was the first one because I misunderstood what she meant at first. What I misinterpreted that

to mean was that the confidential information could only reside in the repository but that's not what she meant; she simply meant that one copy of it should be there.

And then that's sort of what got me going on the question about the server - the Microsoft product that could allow people to manage the digital rights for their files. You know, because one of the nice things about that digital rights management server is that an information provider can at any time remove all rights to a file and make it unreadable even when the files are dispersed to other people's computers. So I'm getting a little technical here but that's - it's that first bullet that sort of got me going in that direction.

And Warren gets a gold star for close reading of my question. But I still don't - I did talk to a friend of mine who sells those products and I don't think they're terribly difficult to stand up. It turns out that that's pretty embedded in the standard Microsoft server environment. And so if we wanted to go after something like that I don't think it would be hard for the sub groups to use it.

So anyway going once, going twice on this particular addition. I liked it a lot but if you have an issue this would be a good time to raise it. Okay, glad you like it too. I thought it was really neat.

The next part that I added is this part and it's pretty subtle in there so let me highlight it. Cheryl raised the idea on the last call, which again I stole - I'm big on stealing people's good ideas - that we might have proxy members in these sub groups, someone like (Paul Vixie) who volunteers to be the intermediate trusted third party between an information provider and the sub team so that the anonymity of the provider of the information could be preserved.

And I think that those proxy participants needed to be acknowledged in this document and this seemed like a good way to do it. So it's partly to clarify how the members are selected but it's also partly to get that idea into the - into the draft. So thanks for that one, Cheryl.

And then the final one is the clarification of the vouched-ness issue, which I know has been contentious. Stop that. And so I added some clarifying language to that part of the document that simply says - clarifies that you don't have to keep the same two people vouching for you; you just need to have two at any given time.

So if someone drops off you can scurry around and find a new person to be your official voucher and you're all set. That was a clarification that came up on the call - I think Jim Galvin mentioned it. And so I typed it in in a hurry and then came back and revised it just a bit. So those were the three refinements that happened between last week and this week.

I think that there are two questions. First let me pause and let people comment on these refinements and then the second question after that is to take a pause and see if people are comfortable with the whole document now. But let me do the first one just take a stop and see if there are questions or issues with these three changes that have gone into the draft since last week.

Good deal. Okay then the second one - and this is really the super important one - is are we close enough that we can call this one a preliminary consensus draft? And then what we'll do we'll publish it as such to the list and give people a notice that next week - on next week's call we'll hopefully get to final consensus on this. At that point we'll publish it.

Is there anybody who's uncomfortable with that idea? Rosella fell out of the room. Julie's good. Cheryl's all good. Cool. Last chance. Don't want to rush but it would be great if we were comfortable with this.

And, you know, I think this is a pretty substantial deliverable. I know that it's painstaking and picky but I think it was Chuck Gomes when I called him

about - just to get clarification as one of the charterers Chuck and Keith Drasek were on the call.

And Chuck said look, you know, you have to have this worked out before you go into the group because it's too hard to work it out afterwards; it's too hard to work it out in the middle of it. So I think that this is really helpful to have thought through in advance.

Well great. I was budgeting a little more time for this than we took so I think I'm going to quit while I'm ahead and say that at least for me that's all I've got. Go back to the picture; so describes our work sometimes.

Nathalie, I think you can cut off the recording and we'll wrap up the call for this week. And I'll go drive some of those changes in and we'll reconvene a week from today. Thanks very much, folks.

Cheryl Langdon-Orr: Thanks, Mikey.

Nathalie Peregrine: Thank you, (Ricardo), you may now stop the recordings.

Man: Okay thanks Mikey.

Man: Bye.

END