Transcript
DNS Security and Stability Analysis Working Group (DSSA WG)
22 December 2011 at 14:00 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 22 December 2011 at 14:00 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-20111222-en.mp3
On page: http://gnso.icann.org/calendar/#dec (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)
- John Levine (At-Large)

ccNSO Members

- Takayasu Matsuura, .jp
- Katrina Sataki, .lv
- Jörg Schweiger, .de (co-chair)

NRO Members

GNSO Members

- Mikey O'Connor – (CBUC) (co-chair)
- Rafik Dammak, GNSO
- Don Blumenthal – (RySG)
- Greg Aaron – (RySG)
- Forest Rosen GNSO
- Scott McCormick (IPC)

SSAC Members

- Jim Galvin (SSAC)

Experts:

- Scott Algeier

ICANN Staff:
Bart Bosinkel
Julie Hedlund
Patrick Jones
Nathalie Peregrine

Apologies:
Luis Diego Espinoza,.cr
Rick Wilhelm, Network Solutions
Nishal Goburdhan (NRO)

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

Nathalie Peregrine: Thank you, (Tim). Good morning, good evening. This is the DSSA call on the 22nd of December, 2011. On the call today we have Takayasu Matsuura, Don Blumenthal, Greg Aaron, Rafik Dammak, Cheryl Langdon-Orr, Mikey O'Connor, Scott Algeier, Scott McCormick, Olivier Crépin-Leblond, Jim Galvin and Forest Rosen. From staff we have Patrick Jones, Julie Hedlund, Bart Boswinkel and myself, Nathalie Peregrine.

And we have apologies from Rick Wilhelm and Luis Espinoza. I would like to remind you all to please state your names before speaking for transcription purposes. Thank you and over to you, Mikey.

Mikey O'Connor: Thanks Nathalie. As always working complex - I think we've got about every bell and every whistle in Adobe Connect in action today and Nathalie pulls it off every week to save us.

I'd like to welcome you all to the December 22 DSSA meeting and holiday party and note that we've actually got the highest attendance we've had in a month I think. So it's great to have you all here.

The first thing is to just take a moment and ask if people have an update to their statement of interest. And Scott is a new member and I'll kind of take a small detour and clue Scott in about this. In the ICANN world we have a requirement that we all sort of tell what our involvement in these working groups is.

And if Nathalie and/or Gisella or Glen or somebody hasn't already clued you in about that why don't you ping me after the meeting and I will fill you in all that because it may sound a little mysterious. But you're off the hook this week and we'll pick this up later. But anyway anybody else got any changes to their statement of interest? Okay.

Next order of business is I'd like to just briefly Scott Algeier and give him a chance to introduce himself actually. Scott came to us through an introduction by Patrick Jones. And Scott and Patrick and I visited right after the call last week. And then the leadership group visited about this on Monday and we are welcoming Scott with open arms.

Scott will tell you a bit about his background. The thing that really intrigues me a about Scott is that in addition to knowing an awful lot about security he's also been through a security assessment for the DNS before. And heaven forbid that we would actually have knowledge in the process to help us out. So I'm pretty darn delighted to have Scott join us. Scott, do you want to just take a minute and tell us a bit about yourself?

Scott Algeier: Sure. So thank you. So I'm the Executive Director of an organization called the Information Technology Information Sharing and Analysis Center. And what we do is we provide a forum for companies to share information about threat and vulnerabilities that they're seeing on their networks as well as kind of protocol issues that might be impacting multiple vendors.

But where I think - in August 2009 I was part of a - I was the private sector chair of a group that released the - what we called then the IT Sector Baseline Risk Assessment. And this was a two-year effort to identify threats to the IT infrastructure itself as opposed to looking at corporate networks. And we were trying to take this at a US level which is obviously hard to do since it's a global environment.

So what we did is we identified specific critical functions that the IT sector provided. And one of them was the DNS - was providing DNS services. So it was through that I guess two-year effort that we developed a methodology to develop ways to access risk through each of these functions.

We ended up using attack trees. And the results of the work are public and I'm happy to share them - share the link with whoever is appropriate to share the link with so we can look at the method so people have an understanding of what the methodology was.

And my expertise is not in DNS itself, I mean, there's - I'm at best a very high level generalist but I think really what I hope to do is listen in and help contribute on the methodology if I can. So I appreciate the opportunity and I look forward to talking with you all.

Mikey O'Connor: Thanks Scott. As you'll see in the chat Jim is ahead of you in terms of posting the link to the report. I should have done that to the list; I didn't even think about it.

One of the things that we do in these is we post these chat sessions to our list so anything that goes into the chat is pushed off to the worldwide Internet unless somebody screeches and says no, no don't post that. But there's a link to the report. And it's quite a fabulous piece of work. I've had a chance to skim it. I'm planning to steal bits of it as we go. And it's great to have you here, Scott.

Scott Algeier: Well thank you. And I just want to - before you go I just want to acknowledge that the work that we did was a joint effort with industry and government. We had in total I think about 70 subject matter experts from industry and US government participate. And to give credit where credit is due Patrick Baggs from the Department of Homeland Security was my co chair on this effort.

Mikey O'Connor: Oh fabulous.

Scott Algeier: Yeah, so thank you.

Mikey O'Connor: Okay. Onto the event - the main event of the day which is continue chipping away at our analysis using the NIST methodology. On reflection I - you all were pretty kind to me in terms of how that last call went but I decided that it didn't go very well.

And one of the things that I realized is that going through those spreadsheets wasn't nearly flexible enough for what we ran into. And so I'm reverting back to the mine mapping approach with the thought that we'll collect the same kind of information but we'll collect it in a way that's a lot easier to sort of improvise as we go.

And then we'll collapse it back into those sturdy tables which are much easier for people to understand in a final report. And so what you see on the screen right now is my first try at a modified version of what we were doing last week.

The big criticism I think of the process we used last week is that we were only looking at threat sources; we weren't looking at threat source event - threat event pairs. And as a result we got pretty wrapped around the axle on evaluating this stuff.

And so what I'd like to try today - and this is in the continuing tradition of incremental improvement until we get it right - is we'll do these in pairs rather than one at a time and see if this works better.

And so the way we'll do this is we'll take a threat source - I think we'll stick with our own favorite, configuration errors. And we'll match a series of threat events with the threat sources. And then we'll do our little evaluation of the three dimensions.

You'll note there's a new dimension that came in during the leadership call that we're going to evaluate. And we'll see how this goes. I'm hopeful that this will be easier for us. It may not be easier in the less work but I think it will be easier in terms of being able to arrive at agreement.

So let me show you a real example. Here's our threat source, a configuration error by a privileged user. And I've just started a list of threat events based on the call that we had last week. And then what we've got behind each one of these is two of those three because Bart came up with this one.

Let me just add this too. And now what we've got is our three little dimensions where in the case of a configuration error in a major zone file, Com, Net, UK, De, so on, what's the range of impact.

And what I’m hoping to do is capture the difference between a major zone file let's say lesser zone file. I'm going to cut in and out for a minute because my phone is ringing but I'll be back.

So before we dive in does this make sense to people or shall I go ahead and just do some of it and then we'll try and make sense out of it then? Maybe that's the thing to do.

So we have our - on your screen we have our traditional poll. I've also thinned out the poll a little bit. I think we got into a little bit of trouble because we had too granular a set of choices; we had 1-10. And I've thinned it back out based on the layers in the NIST methodology.

And you can see those layers down in the lower left corner of the screen. And so when you're saying 10 what you're really saying is a sweeping impact involving almost all of the DNS. That's the translation.

So I think what I'd like to do is just try this today because I'm learning too. And if it works well then this is what we'll be doing for the next probably quite a few meetings because we have a lot of these to get through. And if it doesn't I'll learn some more.

So you can see the poll. And this is the one we're working on. And so I'd like people to just go ahead and use the poll which some of you have used and some haven't. But if you click on one of those numbers it will anonymously put our opinion up there on the screen.

And we'll just sort of see sort of what kind of results we get if we do it this way. So go ahead and answer the question, "What's the range of impact of a configuration error of a major zone file?" And we're getting our first votes coming up. Getting pretty good consensus around 8; a really good consensus.

One person who feels it's even stronger than that. Now what I'm going to do in this version of the process - we're not going to try and actually get to consensus on this. What we'll do is we'll get that first round of votes up like we've got now.

We'll have a conversation about why people feel the way they do. We'll let people modify their votes a little bit. And if we come to consensus great; if we don' I'll just record it because that was another thing I think I did wrong on the last call was to try to drive too hard to get to absolute consensus.

The TLD servers would be - no they would not be the root servers. That's another one that's coming for us; that's a very good question. But this is the

TLD server rather than the root zone itself. Yeah, zone servers as Olivier is saying. That's a good clarification though.

So this would be if somebody misconfigured Dot Com and Dot Com went away what would the impact of that be. And oh there's my...

Cheryl Langdon-Orr: Why is why - it's Cheryl here for the record - which is why I'm hitting in the 8 because, you know, CCs would still be although limited.

Mikey O'Connor: Yeah. Right. Oh for heaven's sakes all of my god damn server stuff is going away. Sorry about blanking your screen like that.

Cheryl Langdon-Orr: Well you were having a winter solstice moment I thought.

Mikey O'Connor: Yeah it was - I should just make the habit of shutting down all the other applications on my laptop before I do this because they always choose our meetings to misbehave.

Okay so what I'm hearing - and here's what I'm going to do is I'm going to document it this way. I'm going to say that there was one vote for the very top most and seven for the next...

((Crosstalk))

Mikey O'Connor: Pardon me?

Cheryl Langdon-Orr: You've got a one on one that needs to be zero.

Mikey O'Connor: Oh thank you very much. Thank you, thank you. Okay now I'm going to skip the Whois impact for a minute and I'm going to go to the - essentially the likelihood although in the NIST methodology they call it relevance to the organization. I don't really know why but I'm going to stick with it for a while.

And this scale is - have we seen it? Has somebody else seen it? Has somebody reported it? Is it predicted, etcetera. And so I'm going to clear the little poll and let you cogitate about that for a minute. And we'll use the same - the nice thing about - you have to ignore - I think I'm going to just - don't know if I've got another...

Jim Galvin: So, Mikey...

Mikey O'Connor: Yeah, go ahead.

Jim Galvin: ...this is Jim Galvin. I'm not sure I understand the question that we're voting on in this case under this relevance to the organization.

Mikey O'Connor: So the - again the methodology has sort of two dimensions to this which says, you know, what do we think the impact is; that's what we just did. And then the other thing that the methodology asks is how likely do we think this is going to happen - is going to be? And the way that the...

((Crosstalk))

Mikey O'Connor: Go ahead Cheryl.

Cheryl Langdon-Orr: I was just going to say it's a likelihood question. We knew we were going to have tweak the nomenclature in some of these branches to suit the global impact which we're looking at because this is design for subsets normally.

Mikey O'Connor: Yes. Yeah that's right. It's really I think designed for primarily an organization level.

Cheryl Langdon-Orr: But could - I know it's annoying - well I'm allowed to be because it's me.

Mikey O'Connor: Yeah, that's right.

Cheryl Langdon-Orr: It's my job isn't it?

Mikey O'Connor: Yeah.

Cheryl Langdon-Orr: That and to stop you mumbling. Could we sort of make some little side notes somewhere - don't know how and where and whatever, I know, sneaking in another color, but something like relevance to the organization. That's one that needs a post think about edit, make it puce or something so we come back to those words because we're going to have exactly the same issue as having to explain ourselves all the time otherwise.

Mikey O'Connor: Yeah I'll put it in here and I'll give it, you know, the only problem is I'm a guy and I don't know what the word puce means so I'll put...

Cheryl Langdon-Orr: Just pick any yucky color that works for you in the sort of (unintelligible) apricot zone and that'll be fine.

Mikey O'Connor: Okay. I get that. Okay let's see if I can make this light enough that I can actually read it. There we go. So what if we said - what if we just changed this to likelihood?

Cheryl Langdon-Orr: Oh that's even better.

Mikey O'Connor: If I can spell it. I'm not terribly smitten with the notion of relevance to the organization. And...

Cheryl Langdon-Orr: Neither am I.

Mikey O'Connor: So - and then the other thing that I’m not terribly smitten with is whether this scale is worded right.

Cheryl Langdon-Orr: Yeah well the - Cheryl again for the record. The concern, etcetera, etcetera, you know, it's - we're crystal ball gazing and they're trying to scale it to a known set of values and a possible set of values.

Mikey O'Connor: Yeah. And, you know, I think that this scale might work. I mean, if we said...

Cheryl Langdon-Orr: If we just - sorry, Mikey. If we just remove from out of those, you know, the scaling the by the organization and...

Mikey O'Connor: Oh just take that clause off of each one.

((Crosstalk))

Cheryl Langdon-Orr: Yeah just take the clause off and I think some of us could maybe feel more comfortable.

Mikey O'Connor: Yeah, I agree.

Cheryl Langdon-Orr: I could live with that.

Mikey O'Connor: I can live with that. Anybody else got howls of protest as I chop these off? A good chance to just leap in while I'm not looking at the Adobe room.

Cheryl Langdon-Orr: This is Cheryl I'll just go ahead. If ever you'd share the edit-ability see we could all have fun now.

Mikey O'Connor: Okay. Let's see. So can - what if we do it like that and then we'll take our little action item away and we'll try it this way.

Cheryl Langdon-Orr: Perfect, perfect. But you'll end up having to clone that so I'd copy...

Mikey O'Connor: Yeah.

Cheryl Langdon-Orr: ...a lot.

Mikey O'Connor: Yeah, cloning is easy. I can - it's the beauty - one of the things that was driving me crazy about the spreadsheets was that they're so hard to edit on the fly like this. So all right we're getting some votes on our new scale. One person is saying possible; a couple people saying more than possible, predicted. So weigh in with your opinions. And...

Jim Galvin: This is Jim Galvin. I think predicted for me, you know, has a connotation of expectation which is different than possible. And so I'm the one vote on the possible side not the predicted side.

Mikey O'Connor: And that's perfect; that's exactly what I was hoping people would do is is they...

((Crosstalk))

Mikey O'Connor: ...outlier explaining why. And...

Jim Galvin: Yeah. I mean, I suppose I could go for predicted if we really want to - I'd be interested in hearing what other people think of in their sense of what the words mean and where they want to go. I mean, it certainly is not anticipated in my view.

But I look at major zones and I think that, you know, those are people with major resources if you will. And so they're supposed to have a lot of stuff in place to prevent this kind of thing, you know, this particular kind of threat specifically.

I mean, accidents can certainly happen. There have been a few examples of those which is why it's possible. But I wouldn't say it's predicted just for that reason. It's not the kind of thing that happens because you don't expect these people to have that kind of problem.

Cheryl Langdon-Orr: Cheryl here for the record. Jim, your rationale is exactly why I leave it as predicted and head away from anything like an anticipated. So using almost the same rationale we're just sitting it at different risk levels I guess - likelihood levels and that's okay; that's good.

Mikey O'Connor: Well and I think that what this will do is this will send us a clue later on in the analysis that says we are probably going to put this one fairly down a list because of this likelihood thing. And we can certainly come back and do a rationale as to why.

Cheryl Langdon-Orr: But a low likelihood. Cheryl again for the record. A low likelihood and a somewhat more extensive if not bordering on devastating outcome still needs to be figured in and this is the way you do that seeing the difference between...

Mikey O'Connor: Right.

Cheryl Langdon-Orr: ...the outcome to the risk or threat and the likelihood.

Mikey O'Connor: Right. Okay last chance. I'm going to go ahead and record what we've got to say at this point. And move onto who because - this was actually Bart's contribution on the leadership call on Monday which was, well, you also have to tell us who.

And I got this - this is a list from the very recently published Internet ecosystem paper that I think ISOC just came out with, I'm not sure. And I just realized that I don't have a scale. Oh let me count; 1, 2, 3, 4, 5, 6, 7 - 1, 2, 3, 4, 5, 6. Argh. Okay I need to create a new poll so there will be a short pause while I do that.

Cheryl Langdon-Orr: Yeah, you see I'd have gone the other way I would have just lumped businesses and organizations together or individuals and businesses together and thought, you know, there you go.

Mikey O'Connor: Oh that's nice. I like that. That makes it a lot easier. Okay we'll go back to this one.

Cheryl Langdon-Orr: Because this is an organization - we're not looking at scale. It could be a micro-business or, you know...

Mikey O'Connor: Right.

Cheryl Langdon-Orr: ...multination, multi-global NGO and a bank I'd stick in, you know, pretty much the same risk level of the Whois, you know.

Mikey O'Connor: Yeah.

Cheryl Langdon-Orr: There we go.

Mikey O'Connor: Okay so now we're down to six. So for the next meeting I promise I will have a scale that actually reads this way on the poll. For now I’m going to trust that all of you can map into this.

So can - oh but this poll also doesn't - oh this poll is terrible because it also doesn't allow multiple choice. I need a new poll. Okay tell you what I don't want to waste time.

Cheryl Langdon-Orr: Multiple, yes, of course you would have to.

Mikey O'Connor: Yeah because you can only vote for one thing. So this is terrible. All right so we're not going to do this today; we'll come back to this one. Let's just do it on the call. Let's just do it on the call. On a major zone file going away because of a misconfiguration. Is there anybody on this list that is not impacted? J

You know, my sense is that this is particular one everybody is impacted. And so to finesse this for today let's just do that. Is there anybody that disagrees with that approach?

Jim Galvin: So not impacted means vote zero?

Mikey O'Connor: No just tell me on the call because the poll is in Minnesota terminology horked up. There's no way that you can actually vote on this particular issue with the poll because it's a single thing.

((Crosstalk))

Mikey O'Connor: So if you want...

((Crosstalk))

Mikey O'Connor: ...go ahead.

Forest Rosen: This is Forest.

Mikey O'Connor: Yeah, go ahead.

Forest Rosen: Are we concerned with fragments of the DNS alternate routes in other words?

Mikey O'Connor: Not on - we are but not on this particular conversation. That one is going to show up in a different threat source.

Forest Rosen: Right because if Com is down and I, a user, never have an experience with Com it doesn't matter to me.

Mikey O'Connor: Right, right.

Forest Rosen: So it is not as widespread or ubiquitous as we might think because there are pockets where users would not be affected.

Mo: Yes that's true. But I think on this particular one we're not describing the pockets that aren't affected we're asking the question whether any, you know, whether any or all of these would be affected by a major zone file going away. And my sense is that they would.

Forest Rosen: If they're consumers of the TLD...

((Crosstalk))

Forest Rosen: ...in question.

Mikey O'Connor: Yes. And these are major - these are major zones rather than lesser zones which is coming up in our conversation.

Jim Galvin: Right, so this is Jim. Jim Galvin...

Mikey O'Connor: Go ahead, Jim.

Jim Galvin: And I think the key phrase in what he just said there was, you know, pockets of non-impact. And I think that, which we'll get to here in a moment, is the distinction between major zones versus lesser zones. I mean, it's a major zone because it is expected to be touched by the majority, you know, pretty close to - well a very large majority let me just say that of the user community for any definition of user.

But there will always be pockets that are not. And I think that's the difference between major and lesser is those pockets how big they are or how small they are. And in a major zone they're smaller; in a lesser zone they're larger. That’s my thought anyway.

Man: (Unintelligible). I'll capture it.

Man: Right, and I think that's the point I was trying to make, is that it's not (bullion), it's no that everybody is effected or not.

Man: Right. Yes.

Man: It is more (puristic).

Mikey O'Connor: That's a good thought. Let me capture that too. I'll put that in as a - I'll organize it like that. Okay. (Olivia), go ahead. Sorry, just came back to the chat room.

(Olivia): Thank you Mikey. (Olivia) for the transcript record. We were looking at the impact, who is impacted, and I just wonder about one particular thing which is actually related to our actual mandate. There is a certain issue of perception that is involved (with) this.

And certainly one thing which we are looking at is to I guess correct a certain perception maybe or find real facts behind perceptions to find out if really the DNS is in trouble or not. And so the idea of perception on this thing, it might be a major zone, a minor zone, it might be a huge new GTLD zone or it might be a very small one.

Whatever happens, if one actually fails, if there is a failure there, no matter how many individuals will be affected, it will still make headlines and at least in the early days.

So the perception of it is equally as bad whether it is a small or large zone in my opinion. Thank you.

Mikey O'Connor: Thanks (Olivia) and I think that that kind of gets back to the range of impact issue as well which is that this would clearly be a pretty big black eye in addition to the technical impact. There would - you know, and so then the question becomes do we need another category at this level which is nature of impact.

And then put the perception thing in there but also - I don't know. I - the trouble with this is that the tree gets so branchy. I worry about that. Any thoughts on that one, what we'd do with (Olivia)'s point? Maybe we'll leave that as an action item to figure out.

Because it may be that there's a place in the methodology which I still don't know well enough.

(Olivia): Mikey, it's (Olivia). May I?

Mikey O'Connor: Sure. Go ahead.

(Olivia): (Suggest) - thank you. (Olivia) again for the transcript. I actually mentioned this, not to make the tree larger but to try and simplify it somehow because I see here that we are looking at the range of impact and the, you know, how much impact would it have and trying to classify it in this way.

And I'm thinking, well, for any failure, yes, the technical impacts might be quantifiable but the qualitative impact, the perception impact, is probably due to the fact that there's so much publicity going up around it.

It's probably going to be pretty high at any case. So I wondered whether we needed to actually go through such detail to look at the exact range of impact or extent of impact.

Mikey O'Connor: I think we need to do that in order to pick the ones that we ultimately are going to come back to the community and say we're quite concerned about. We may come back with some of these and say, "I don't think this is such a big deal."

Oh by the way, somebody is listening on their speakers and has their phone unumuted. That's why we're getting a little bit of echo right now. I can hear every word coming back in my ear. That's the difficulty. Joerg, go ahead. Sometimes it takes Joerg a minute to get off mute.

Joerg Schweiger: Okay, can you hear me now?

Mikey O'Connor: Yes.

Joerg Schweiger: So Joerg for the transcript. I'm a little bit worried about direction we are currently heading toward. I think we are concerned with technically impact. At least this is the (sculpting) we have been tasked with.

And I find it very difficult to include something like perception. I do realize that perception may be a point but we're just not concerned with perception. And so for sure, perception would be very, very different depending on who you really ask.

If I would be involved in a configuration (error) that would virtually take off my zone from the Net, I'll be - I would be really, really, really concerned. Whereas, if you ask me if, let's say, FX for example because it's just new and it came to my mind, if there would be a configuration error in the FX zone and FX would be gone for two hours from the Net, my perception is I don't care.

Sorry about that, but I think that makes clear that perception very much depends on the perspective you're currently in and I doubt that we would ever get a unanimous vote for perception.

Mikey O'Connor: Let me take an action on this one to figure out what to do with this. I - it's a good puzzle. I don't...

(Scott): And...

Mikey O'Connor: Go ahead.

(Scott): I'm sorry Mikey. It's (Scott). So we kind of grappled with this a little bit as well when we did our risk assessment and we kind of put it under the - look at this perception and also in the context of public confidence, right.

Does the public lose confidence in the infrastructure and, you know, does the government or do governments also likewise lose confidence and, you know, even - we grapple with this concept that, you know, even though it may not be a big issue to our company or it may not be a big technical issue to the infrastructure itself, it was perceived as a big problem, it could undermine confidence in both the infrastructure itself.

It can undermine confidence in the companies who operate that infrastructure in the minds of the public.

Mikey O'Connor: Thanks (Scott). That's exactly why I was so glad to have you on our - in our gang. Anybody else want to ch- (Olivia), is that a new hand or an old hand?

(Olivia): It's a new hand, Mikey.

Mikey O'Connor: Go ahead.

(Olivia): Thank you. It's Olivia for the transcript. Actually just following up on what (Scott) has said, loss of confidence indeed. The reason why we're here is a perceived loss of confidence. So in a way I think that, as long as we mention that perception wise, many of these things that we're evaluating might be seen by the public as being - or perceived as being particularly important and journalist, et cetera, or the press and all this, we will be looking specifically at the technical stuff. Hearing what Joerg has said earlier, I do agree with that as well.

Mikey O'Connor: Okay, so what we could do is - maybe what we can do is in- damn it - sorry. Sorry for the screw up and the cursing - is in a way, this issue applies to almost every single thing that we're going to discuss.

Man: That's correct. Yes.

Mikey O'Connor: And so rather then evaluate it at every branch in the tree, the - how about that? What if we put it in the introduction to what we're talking about so that we can acknowledge that while we fo- you know, that while we focused on technical issues, that there's also a very likely loss of confidence if any of this major infrastructure fails and finesse it like that? (Olivia) is typing. That was mine. Yes, I know you didn't. That was...

(Olivia): I was basically saying the same thing as you just now Mikey. Thanks. Okay.

Mikey O'Connor: Yes. Yes, let me just steel that out of the notes. Okay, so I think that we've gotten through one of these today. I was hoping to get through more but - let's try another one just to see how it works. So let's do - instead of a major zone file, let's do a lesser zone file. Same deal.

Range of impact is our first poll- oh Joerg, I'm sorry. I wasn't looking at the screen. Go ahead. He may still be muted. I still...

Joerg Schweiger: Okay, got it now.

Mikey O'Connor: There we go. There you go. Now I can hear you.

Joerg Schweiger: Joerg for the transcript. So if we do acknowledge that we think that we have a - let's say political impact or the impact of trust in the infrastructure of the parties involved running the infrastructure. What comes to my mind is what are we doing that? So we completely acknowledge that the perception is a thing we do have to look at.

But are we about to do anything against a misperception or a perception that is not in favor of the operations we are currently conducting? So it's...

Mikey O'Connor: I...

Joerg Schweiger: Any technical reaction to that?

Mikey O'Connor: There's a whole section of the methodology that's coming that's going to talk about mitigation and I think that that's a place where that sits, is that when we get to the threats that we're very concerned about especially we'll focus on mitigation that's already in place, controls, et cetera, et cetera.

And so I think there's a pretty broad opportunity to document what people are doing both today and maybe even should be doing more of tomorrow that's coming up.

But I think what the methodology is trying to do is break some of this into smaller bites because if we try and go all the way through the whole analysis of a single branch of threat tree, we sort of get lost in the weeds.

And so I think that one I'd like to lobby. We just wait and I think when we get to the mitigation part of this discussion we'll be able to document that. Is that okay with you Joerg?

Joerg Schweiger: I'm thinking about it. Probably I'll rephrase it later on. It's okay for now. Thanks.

Mikey O'Connor: Okay. Okay, and (Olivia) said in the chat mitigation plays a large part in approving perception, so that's sort of a related point. Okay. Let's see if we can do one a little bit faster. Let's do our lesser zone file range of impact conversation. Go ahead and just bang your thoughts into the poll, sort of get what people’s reactions are. Have a quick conversation to tune those reactions and then move on.

So a lesser zone file is like the one that Joerg was talking about, a small zone, either a small CC or a small GTLD. And it goes down due to a - still a misconfiguration by a privileged user.

And again, we’re sort of clustering in the minimal to limited. Anybody want to argue one way or the other on that one? (John Levine) says if dot travel went away, would anybody notice other then me? Probably not. That’s a good example of a lesser zone file. I’m sorry.

To all of you dot travel people who are listening to this recording, I apologize. That’s funny. Okay, I think I’m going to do the same thing. I’m going to just document it that, you know, most of us are thinking that it’s limited. I’ll record the seven folks that feel that way and a couple people feel that it’s truly minimal.

And again, now what I’m going to do is steel our likelihood range. Oops, not that way. Take away the relevance one. Let’s talk likelihood for this one. Now I got a bunch of editing to do. Let me clear the poll so that you can - while I’m tinkering you can go ahead and fix this.

So again, lesser zone file, what’s the likelihood that this is going to happen? And we’re getting pretty strong divergence. So folks should be prepared to argue one way or the other. Again, this is one that I would personally expect to be more likely just because some of these organizations are quite small, not terribly well resourced, et cetera, et cetera.

So I’d be interested in hearing the arguments for why even a lesser zone file is quite unlikely. Does anybody want to come in on that? (Olivia), go ahead.

(Olivia): Thank you Mikey. I'll just reiterate what you just said. It's (Olivia) for the transcript. Smaller zone file, smaller amounts of resources. Fly by night cowboys. More likely to fail. Okay, maybe not that (plastic) but it seems to be that you're everyone's mental linkages then they have - generally would make us think of smaller operation, is more likely to have technical problems.

And it's not always the case. In fact, smaller operations are sometimes a lot more careful about how they run their things. So it's a tough one. Thank you.

Mikey O'Connor: I don't think it's an issue of care. I think it's an issue of resources primarily. One of the things that I would expect to see in a really large zone file, is more programmers, more analysts, more time available to develop technical controls around this.

((Crosstalk))

Jim Galvin: So it's Jim. I...

Mikey O'Connor: ...resources. Jim, go ahead.

Jim Galvin: I think, Mikey, what you're suggesting is more automation.

Mikey O'Connor: Yes. Yes.

Jim Galvin: I think that, yes, larger automation - automation - larger operations tend towards greater automation and thus once you get it right, it tends to stay right. Or at least you have different kinds of failures that can happen. And I mean, your automation can always fail too. But I see that as a distinction between smaller and major zones also.

Mikey O'Connor: Yes, right. (John), go ahead.

(John): Yes, I think this is actually two questions. I mean, a lot of the small zones outsource the action operations. I mean, without travel, I believe it's just as reliable as dot com because it's run by VeriSign.

Mikey O'Connor: Yes.

(John): And I think you're more likely to see problems in, you know, a small country that doesn't have a lot of expertise but coupled together, a couple of name servers run by their friends.

Mikey O'Connor: Right. And maybe our definition needs to change so that we say a lesser zone file that is not outsourced to a major...

(John): It's not the size of your zone file. It's the size of the operator.

Mikey O'Connor: Yes.

(John): So - and we can have discussions somewhere else about, you know, like dot museum which is a tiny operator but (carry is) very competent.

Mikey O'Connor: Right.

(John): But (unintelligible) those.

Mikey O'Connor: What if we did that modification to our (threat) event? What does that do to the voting? So now we're eliminating essen- you know, we're essentially narrowing this use case to only those where there are less likely to be tremendous resources.

We've still got pretty good dispersion. I'm not going to beat this to death but I would like to hear from some of the three folks on that.

Jim Galvin: So this is Jim. I have a question.

Mikey O’Connor: Sure. Go ahead.

Jim Galvin: So for those who are voting eight, maybe this again is just some word smithing that’s important here, but we should presume that the comma phrase there is not present, right? So the range of impact, the extensive is, again, I guess it depends what the user community is.

I think what’s funny even about lesser zone files is the range of impact is significant and sweeping for those who are a part of that zone, so pick a small country, right? That country goes down and you have a problem with that zone file, that country actually cares a great deal. And it’s a huge and major crisis problem for them. For the rest of the globe, it’s probably insignificant.

Mikey O’Connor: Right.

Jim Galvin: And I think that’s an important distinction to make in this range of impact. You know, previously when we were talking about major zones, it was sort of easier to suggest that the impact would be extensive because it was also pretty clear that it matter to everybody whether you were in the zone or not.

When we’re talking about smaller zones, I think there’s great importance or significance that goes with being in the zone or not being in it as to what the impact really is.

Are we judging the impact based on the global effect or judging the impact based on the user community of the zone? That’s my question.

Mikey O’Connor: The way we - yes, that’s a good question. And it’s sort of the reverse of the discussion we had on the first one which is in this case, it’s, you know, it’s basically the opposite of this I think. Does that capture the thought that you’re coming at us with there Jim?

Jim Galvin: Yes, I think that's at least enough to...

Mikey O'Connor: At least enough of a reminder.

Jim Galvin: Right, enough of a reminder. Thank you.

Mikey O'Connor: Yes. Okay, so I'm going to ca- oh, Joerg, go ahead. I'll start capturing while you talk.

Joerg Schweiger: Yes let me comment on what Jim just said. I think this, once again, is a question of perception and I think it's very clear what we are concerned with. We are concerned with (the DNS) and even though it might be very true for the citizens of a small country, that if there zone (power) would be affected, they really do care.

But nevertheless, this wouldn't have an impact on (the) DNS as we phrase that. So after this I would doubt that we would be - as this working group, be concerned with that problem.

Mikey O'Connor: I think that's also a fair statement. Jim, do you want to come back on that?

Jim Galvin: Yes, so Jim Galvin here. So Joerg, it sounds like you're suggesting that - you're questioning the people who are voting eight and ten on the impact of this kind of problem because it sounds like you're trying to get us to focus on evaluating this in the context of the global DNS.

And I think I agree with that. But, again, at this point it's important to hear from others here or those who are voting eight as to why they want to vote that way.

Mikey O'Connor: Let me - they're not - Jim, just to clarify, they're not voting on the range of impact. They're voting on the likelihood. When we talked about the range, we tended to agree that this is a fairly limited impact except the caveat that you brought up, but that it's pretty likely. It's much more likely that this is going to happen for the resource issue.

So the (As and Ns) aren't about the range of impact. They're about the likelihood of the impact. Does that make sense?

Jim Galvin: Yes it does. I apologize and I was just a little out of context there but...

Mikey O'Connor: Well, this is how we're all learning how this works, so I can sign up for confusing the hell out of people. Sorry about that.

Man: This is...

Mikey O'Connor: Joerg, go ahead.

Man: I'm sorry.

Mikey O'Connor: Oh no, go ahead. (Scott).

(Forrest): This is (Forrest).

Mikey O'Connor: (Forrest), go ahead. People who don't raise their hand, confuse your co-chair.

(Forrest): Oh I - oh, there we go. Okay. I apologize. I'll use that in the future.

Mikey O'Connor: Yes, no worries.

(Forrest): As a segue into range of impact, we might define the space as all users for the Internet rather then defining them as users that are within the impact space, because users in the impact space are pretty much the buoy and you are affected or not.

Mikey O'Connor: Right. Right.

(Forrest): Okay. But if we broaden the space to all Internet users globally, then we can have more of a meaningful discussion of the range of impact and actually compare it to if we look at dot com, TLD root service is going down. And we can say dot com traffic represents X percentage of global traffic versus some random dot XY small TLD root service as a very small relative percentage of global traffic.

We can have a meaningful comparison because you're only looking at the space of impact. Then, of course, it's 100%.

Mikey O'Connor: Right, and I think that's the caveat that we just put in. I'm going to cut you off, (Forrest), not because I don't like you but because we have, indeed, run over the top of the hour and I need to draw the meeting to a close.

And so for those of you who have to go, go and have a wonderful holiday season. We'll see you in a couple of weeks. For those of you who can hang on for just a minute, I'd like some feedback on whether this process is better or worse then the one I did last week. Any final thoughts? Am I taking this in the right direction? Anything that people can think of to make this work better for us?

(Carol) is saying, "Getting there." That's good. I like that. I will once again, listen to the recording and try and make it better yet. Have a great holiday and we'll see you in a couple of weeks. No meeting next week, so talk to you in two weeks. Bye-bye.

Woman: Thanks Mikey. Bye-bye.

Woman: Thank you (unintelligible) the recording...

END