Transcript
DNS Security and Stability Analysis Working Group (DSSA WG)
09 February 2012 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 09 February 2012 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-20120209-en.mp3
Presentation will be posted shortly on:
http://gnso.icann.org/calendar/#feb

Attendees on the call:

At Large Members
. Cheryl Langdon-Orr (ALAC)
. Olivier Crépin-Leblond (ALAC) (co-chair)

ccNSO Members
. Takayasu Matsuura, .jp
. Katrina Sataki, .lv
. Jörg Schweiger, .de (co-chair)
. Jacques Latour, .ca
. Wim Degezelle, CENTR

NRO Members

GNSO Members
. Mikey O'Connor - (CBUC) (co-chair)
. Rossella Mattioli - (NCSG)
. Greg Aaron - (RySG)
.Rafik Dammak, GNSO
.Forest Rosen GNSO

SSAC Members
Jim Galvin (SSAC)

ICANN Staff:
Julie Hedlund
Bart Boswinkel
Nathalie Peregrine

Apologies:
Mark Kosters (ARIN); (co-chair)
Edmon Chung - (ALAC)
Scott Algeier - expert

Coordinator: ...the call is now being recorded.

Nathalie Peregrine: Thank you (Tim). Good morning, good afternoon, good evening. This is (unintelligible) call on the 9th of February, 2012.

On the call today we have Mikey O'Connor, Cheryl Langdon-Orr, Rafik Dammak, Olivier Crepin-LeBlond, Rosella Mattioli, Jacques Latour, Joerg Schweiger, Katrina Sataki, Greg Aaron, (Forest Rosen) and Takayasu Matsuura. From staff we have Jaime Hedlund, (Bob Sheshinko) and myself, Nathalie Peregrine.

We have apologies from Edmon Chung, Scott (unintelligible) and Mark Kosters.

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

Mikey O'Connor: Thanks Nathalie. I note that while you were calling roll that Jim Galvin and (Forest Rosen) joined. So you can add them to the attendees.

Running quickly through the agenda. We're really going to work on architecture and analysis today. We'll take a moment right at the end to update you on the meeting schedule for our meetings in Costa Rica.

I'll give you a moment to add things to the agenda and/or let us know about changes to your Statement of Interest and then we'll get going. Anybody have either of those things they want to talk about?

Okay. I've actually got the wrong thing on the screen. Typical. Let me get the right thing on the screen. Just a short moment.

I want to take a second - we got started on this last call and got stuck because we didn't have the folks on the call who knew the answers that we were asking - to the questions we were asking.

So before we dive back in to the voting and analysis, I want to take just a quick second to start at the provisioning systems for the root zone. We had a little bit of a conversation about this on the list. And I think that the answer to this sort of looked at those questions is that there is an automated system to provision the root that I think IANA runs. Is that right? Somebody correct me on that.

And then the operators do indeed have different systems that they're in for provisioning. Again, just want to make sure I'm right on that.

I'm seeing - oh, I guess it's just a - so that one is done. The next question that I want to get an answer to - we've been talking about the IANA zone in our analysis. And several people stuck their hand up having not really been on the calls and said, "What are we talking about when we talk about the IANA zone? Because if it's indeed the same as the root zone, then that's a duplicate branch in our tree." So is there a different file that is actually the IANA zone as opposed to the root zone or is this a duplicate?

Anybody want to educate your poor co-chair on that?

Jim Galvin: So this is Jim. I'll just comment that I think it's a duplicate. I don't remember the discussion that added it there. So that would by my opinion today unless someone has additional context. There's no such thing that I've ever heard of called the IANA zone.

Mikey O'Connor: That's the kind of answer I like.

Anybody got a different answer than that? Because if it is I'll cheerfully entertain the debate. But if this is really truly a duplicate I am delighted to take it out. It's going once, twice.

Man: Gone.

Mikey O'Connor: Gone. All right, let's make it gone. Terrific. All right, that's very helpful.

Now want to then take us - I'm going to briefly flash this on the screen. This is our spreadsheet where we're recording our votes. And we're soon going to get back to this spreadsheet.

But I want to take you on a quick trip off to a conversation that we had amongst the co-chairs while we were preparing our update for the Costa Rica meeting. In which - I'm raising this issue, but I think I have a reasonable level of agreement that we're sort of up against a difficult problem.

And that is that the way we're doing this doesn't scale and we could wind up spending a very, very, very long time analyzing a very, very, very big threat tree because of the way that we're combining the layers of the threat tree.

What the methodology likes to do is it likes to take a layer of the threat tree at a time -- so like threat events, threat sources, vulnerabilities -- and have the group find the ones that matter. So the little threat events that have -- in this case -- exclamation points by them is the way I'm depicting that.

So that instead of evaluating every single branch of what could be 1000 permutation threat tree, we go a layer at a time and only evaluate the branches that are worrisome. It's not that we eliminate the branches. It's just that we make the choices as we go so that we don't have the threat tree explode.

And I'm going to show you this in reality in just a second because I'm going to flip back to the spreadsheet. And I've now created the spreadsheet with all the permutations that we need to evaluate by voting. I think you'll see what I mean.

I wanted to present this picture to you before I went to the spreadsheet though and show you why I keep on every single call worrying about this.

So let me go to the spreadsheet. And I'm going to, you know, this is our familiar, you know, we're doing one threat source at a time. We've been working on - for a long time we worked on configuration errors. We're now nearly done with business failure of a key provider.

And now I'm going to shrink the spreadsheet so that you can see the whole thing. You can see that's the first half. That little tiny yellow gizmo right there is where we are.

And now I'm going to show you the second half. You can see that we have quite a ways to go if we keep doing this pair-wise comparison like we've been doing.

And on top of that - now I'm going to go back to the normal scale, which you can read it. Another thing that I did is I added a new column which I multiplied the results of our analysis on range of affects times the result of the analysis on relevance.

So 100 would be big range of affect and we've confirmed that this will happen, so that would be a big problem that we would really want to analyze. And a zero would be the opposite. It would be a minimal effect and, you know, either possible or never seen before.

And what I want to call out is that for all the work that we've done we've really only identified one worthy pair so far, which is that if there's a configuration

error by a privileged user that changes a major zone file, that's going to be a big problem and that's one that we've seen before.

And so what I'm lobbying you for is the notion that what we might consider doing is finishing maybe - maybe finish the business failure one today because we've only got a couple/three more to do. Do one more just to get, you know, we can quickly pick another one that we think would be a good one.

And then on the next call try to actually break this back apart and come up with a single number for each of these two kinds of things that we're evaluating and have those numbers available on a preliminary basis for Costa Rica.

I think that that chops out what otherwise will be a month or two's worth of work at a minimum given the number of permutations that we've got in front of us.

And if this was a month or two's worth of work where we were producing a lot of things that we were likely to analyze in subsequent steps I wouldn't be so worried about it. But I think we may be doing a month or two's worth of work. And at the end we will say, "Oh well, none of these are important." I'm just really concerned about doing that.

So that's the context. I don't want to change the way we're working right now because I think that the work we've done is extremely useful for putting that analysis together next week. Because we can kind of look back at our votes and start to draw some, I think, pretty good conclusions.

But at the same time I'm going to continue to push back on the idea that we do every single pair-wise comparison because now I've beaten to death - I think we're headed down kind of a black hole with this.

So that's context. Now we go to work. And if you note the place we stopped on the last call was on the threat source being a business failure of a key provider that disrupts the (DNSSEC) from a major provider.

We fairly agreed that the range of affect could be pretty broad. But we had a pretty good dispersion on the - oh sorry, I'm highlighting the wrong thing here. Take this out. This is confusing. There. We had pretty good dispersion on whether we've seen this before question.

So I sort of want to pick up the voting right here and ask the question again. So the scale that we're going to use is the middle one where a ten would be, "Yes, we've seen a business failure of a key..." No, "where we've seen the (DNSSEC) from a major provider disrupted."

And the examples that we were talking about last week were things like the misconfiguration - I think it was of NASA's (DNSSEC) that knocked out the nasa.gov subdomain. And, you know, it wound up being something that could happen. So we had a fair number of votes at the ten end. And then we had one vote at the one end.

So with that, off we go. We go ahead and sort of indicate what you think the range is all the way from ten -- which is confirmed -- all the way down to zero -- which is not applicable -- or one. We'll get going.

Oh, I note Cheryl's comment. And I'll talk to that while you're voting.

Cheryl Langdon-Orr: We'll get back to that, Mikey, not now.

Mikey O'Connor: Yes. We'll get back to that one.

Cheryl Langdon-Orr: We'll get back.

Mikey O'Connor: I have to kind of invent that conversation and I don't know how it's going to be structured quite yet, but I agree. I think maybe the way we do that is we do a couple/three like we've done with this arrangement and see if we can spot some trends. And if we can, go to the pruning.

But I agree with you, Cheryl. I have to kind of invent how we're going to do this so that we don't do it badly.

Come on voters. I got nothing more for you. Just waiting for people to tell us whether you think this is something that's happened before, that we've seen it, our peers have seen it or our partners. So we're starting to get people coming in around the three range.

Give you just a few more minutes and then we'll go on to the next one. Going once. I'm going to start recording. Two fives.

Cheryl Langdon-Orr: (Because) Mikey, you had us doing relevancy, not range of affects, didn't you?

Mikey O'Connor: Yes. We've already done range.

Cheryl Langdon-Orr: Yes. That's what I thought. Yes, that's fine.

Mikey O'Connor: Yes, yes. We're doing relevance. And I'm going to clear this so that we're - quite so confused.

All right. So the next one is the range of affect -- so that's the scale on the left -- sweeping almost all of the (unintelligible) resources to the DNS all the way down to limited.

But this time what we're talking about is business failure of a key provider disrupting the (DNSSEC) for a TLD zone. So presumably this would be

somebody who - the registry for a TLD zone have a business failure and the range of affect of that in this context.

We're floating in around four, five. Okay. Last minute voting. Up to six. That's the sum of the last one. No, the last one was nine. There are nine, okay. (7, 1, 1).

Ignore the changes in colors. I finally figured out where those are coming from. They're artifacts from the way I built the file.

But, you know, when the number that we type in is red and is the highest one, that means it's probably the same as the first one that we did. Because what I did is I was copying (unintelligible).

Cheryl Langdon-Orr: Okay.

Mikey O'Connor: So if it pops up that the red one is also the highest one in this go-round, that means that we're pretty consistent. And you can see, for example, that up above there was a seven that was highlighted red as well. So that's what's going on.

I didn't realize that that was what was happening until I...

Cheryl Langdon-Orr: I like consistency, consistency's good.

Mikey O'Connor: Yes, consistency is a good thing. Okay, so same drill. We'll clear the voting. Thanks Nathalie.

Now we're on to the relevance question. Same thing. Have we seen a business failure of a key provider disrupting (DNSSEC) for a TLD zone? Has that ever happened? Or can we imagine it happening? Or can we imagine it happening in such a way that it would actually disrupt (DNSSEC)? You know, sort of presuming a lot of things are happening.

Go ahead and ponder that for a minute and then tell us what you think.

Close to 100% certified ICANN pure consensus (for) nine voter comes in at that level. Going once, going twice, just one person who voted and the other ones who haven't voted yet. But I'm not going to wait for you.

Okay. Onto the next, which is business failure of a key provider disrupting critical DNS support files. For those of you who forget what those are, there's the list. Hints, root-servers.net, root's public key resolve or config files. We're not going to do the individual files. We decided we would just say if those support files got disrupted by the business failure of a key provider, what would the impact be of that?

So this is, again, the range of impact question on the left that we're talking about.

We're up to eight. Going once, going twice on those votes which tend to center around (unintelligible).

That one. Okay, clear the gizmo and then we'll move on to the relevant one.

Woman: Hi there.

Mikey O'Connor: Oh, we've got somebody that just said, "Hi there" that's not on mute.

This is the - whether we have seen anything like this all the way down to (conceivable) it's been described by a somewhat credible source, or maybe not even relevant at all.

And the pair that we're evaluating is business failure of a key provider disrupting critical DNS support file.

Stuck at five out of nine. If we can get a few more in there before I tally it. (Joerg) just dropped off and had to come back in again. Maybe that's why our number went down. Welcome back (Joerg).

Okay, we're up to seven. And I think we'll call it seven on that one. I mis-recorded the last one too. Don't really (unintelligible).

Cheryl Langdon-Orr: That's better. Thank you.

Mikey O'Connor: Okay. Next one and last one in this group, which is we're back to the range of impacts question. This is a business failure one again. This time the business failure disrupts the provisioning systems between the registries and the registrars. The result being registrars can't add, change delete zones from the TLD.

Now this one would be - I guess the scenario could be VeriSign goes out of business, abruptly that disrupts the provisioning to put subdomains in the zone. (Go ahead) and vote on that.

We're up to seven. Hanging at seven. It's up to eight. Getting real close, think I'll go ahead and record now. Nine, hey, there we go, full tally. Cool.

All right. Same deal. We'll move over to the question of whether we've seen such a thing happening all the way down to being a possibility or perhaps not even applicable.

...mind me, I'm just tidying up. I was wondering why my little multiplication didn't work.

Okay, so we've got eight. (Unintelligible) that one last straggling vote one time and then we'll go ahead and record this. Recording with (6, 1, 1) starting at 5.

Okay. (Unintelligible) working.

Cheryl Langdon-Orr: Mikey, Cheryl here just before you move on to the new section.

Mikey O'Connor: Sure, go ahead.

Cheryl Langdon-Orr: Thank you. I just needed to get this off my chest at this point. Particularly in those last few decision notes on the business side of key providers. I kept thinking to myself in the current landscape, I was very aware that my answer's might be different in three year's time in an expanded landscape.

Mikey O'Connor: I had that same thought. And I (unintelligible) was...

Cheryl Langdon-Orr: And I just needed to make sure I shared it with everyone.

Mikey O'Connor: No, I...

Cheryl Langdon-Orr: I just feel that we need to - asterisks somewhere that this is here and now analysis.

Mikey O'Connor: Right, and...

Cheryl Langdon-Orr: Not (unintelligible) (gazing) expanded gTLDs by analysis.

Mikey O'Connor: Right.

Cheryl Langdon-Orr: That's the difference (unintelligible).

Mikey O'Connor: I think that what we have to do is in our report that asterisk has to be in the instructions to the people doing the ongoing maintenance of the risk assessment.

Because clearly as things change -- like a whole bunch of new TLDs or a whole bunch of new providers -- as soon as one of those kinds of things shows up, somebody ought to jump back in to this threat tree, change that answer and see what the impact is on the risk.

Cheryl Langdon-Orr: Yes, I mean...

Mikey O'Connor: Hope is that what we'll wind up with is a whole linked set of spreadsheets based on these but arranged a little bit differently. So that if a person could go in and say, "That answer changes now, what impact on the bottom line risk?"

Cheryl Langdon-Orr: A small group probably would as opposed to a person. But yes, I think perhaps it might be just penciled in on the side of a notepad somewhere. We need to pick these up in a recommendation section of their final report.

And again, if we do a full-blown, totally tiered analysis this time -- and I may argue for that yet -- we wouldn't necessarily suggest that needs to be done each time. We could suggest a sort of a faster track -- pardon the pun -- on future analysis. But we also might want to look at periodicity and critical points which would trigger a revisit into parts of the analysis at least.

All right, boss, you can move on now; I've got that off my chest.

Mikey O'Connor: That's a good one. Let me just capture it because this is a good spot to put it.

Cheryl Langdon-Orr: I mean, if it wasn't so heavy, Mikey, Cheryl here again, I could bring my crystal ball to Costa Rica but its volcanic glass so it's a very heavy crystal ball.

Mikey O'Connor: Yeah, yeah. I don't think we need it.

Cheryl Langdon-Orr: We could try looking into the future but...

Mikey O'Connor: I think on that one it's pretty easy to tell what the future is going to look like. Let me add another note in another place because I think that - oops, not that one. Here's where we can also add a note - okay.

((Crosstalk))

Cheryl Langdon-Orr: ...I don't know whether I can answer that but I'll...

Mikey O'Connor: Yeah, yeah and if you could let me know. I've got a couple of things I want to put some money on in the stock market. I'd love some answers to that.

Cheryl Langdon-Orr: Well because while you're making your notes and there's dead air and I hate dead air anyway I can tell you when I do use the crystal ball - and I actually use it in a lecture series, believe it or not, a crystal ball is on a stand - it's a real crystal ball.

And I put a - it up and I get people to look in the crystal ball and there is something underneath the crystal ball that if they look properly they can see. But by putting a dollar or two dollar coin at the base of the crystal ball stand it depends totally on from where you are looking as to what you see.

Mikey O'Connor: Oh.

Cheryl Langdon-Orr: So people can genuinely see one, three, five, seven...

Mikey O'Connor: Oh.

((Crosstalk))

Cheryl Langdon-Orr: ...a lot about predicting the future and that's the purpose of the tool.

Mikey O'Connor: That's quite delightful. Okay we're onto the - a whole new category. And we've got choices at this point. Let me give you your choices as to which one you'd like to evaluate.

Some of these are not like the others. So for example nation states doing an unintentional thing is a quite different threat source than key storage processing network failure. And these two are pretty similar - networking or operating system software failure, application software failure; those are all pretty similar.

Same with, you know, we have a whole bunch of sort of infrastructure threat sources. Then we have the root scaling one and then we have natural disasters which are pretty similar to widespread telecom failures and power infrastructure failures. That's our list of candidates.

And one kind of pruning that we could do is we could say, you know, a lot of those are fairly similar; let's do one of each but not do them all. And if that were the case - too high.

And then this one - when we were talking about this particular threat source on the call that we put it on this list Don Blumenthal, who was at that moment right in the midst of the SOPA debate here in the US, was pretty emphatic that there is no such thing as an unintentional or accidental intervention by a nation state.

And so he was lobbying pretty articulately that there - that this is an invalid threat source and that we should just remove it altogether. So before we actually dive into this one I think we need to pick that debate back up again.

I think when we were describing it, you know, at least I was using SOPA as the example where the legislators were simply ill-informed about the impacts of the law that they were writing.

And that that could be categorized as an unintentional or an accidental intervention as opposed to a government like Egypt shutting down the, you know, the edge servers at their country as being a malicious one.

So before we actually evaluate this one I just want to take a moment to confirm that we still agree that this is one that's valid to evaluate. And I'll, you know, I'll go ahead and start us on this in a few seconds unless somebody throws their hand up and says no, no, no, Don's right, there is no such thing as this.

Not seeing anybody throwing their hands up so I think we'll go ahead and evaluate this one and then I'm sure that by the time we get done with that if we do we'll wrap for the day except for the schedule.

Forest, go ahead.

Forest Rosen: Yes, Forest Rosen. Well what about just changing the language of the threat saying it's an intentional action with unintended consequences.

Mikey O'Connor: Oh that's an interesting idea. I could buy that. Anybody got a problem with changing it that way?

((Crosstalk))

Forest Rosen: I tend to agree with the assessment that action is intentional. I would also agree that oftentimes there could be unintended consequences.

Mikey O'Connor: Yeah.

((Crosstalk))

Cheryl Langdon-Orr: Yeah.

Mikey O'Connor: Go ahead, Cheryl.

Cheryl Langdon-Orr: I was just saying it's the naiveté factor, yeah.

Mikey O'Connor: Yeah and I think that really adds a lot to that description. Okay any - let's go with that just - I'll change this.

All right let's do us some voting; so the first one is the range of effect sweeping all the way down to hardly any at all. If a nation state did something that accidentally disrupted a major zone file what would the range of effect be? This is again, you know, the sweeping almost all of the DNS all the way down to very limited effect.

Cheryl Langdon-Orr: And yet it was Tuvalu versus, you know...

Mikey O'Connor: Yeah, this is the...

Cheryl Langdon-Orr: ...some other larger nation state...

Mikey O'Connor: Right, this is the major zone file as opposed to the next one...

Cheryl Langdon-Orr: Yeah.

Mikey O'Connor: ...which is the smaller zone file.

Cheryl Langdon-Orr: That's right.

Mikey O'Connor: So this would be, you know...

Cheryl Langdon-Orr: A serious lump of (spit).

Mikey O'Connor: Yeah, this would be a big bite out of the domain name space if this happened. Sort of homing in on 5; got eight people there. Going once, going twice for our nine - there we go, we got nine, right.

Okay now we'll do the relevance one which is the confirmed all the way down to possible. I lost the scale on the middle one at the bottom there, the relevance scale.

((Crosstalk))

Cheryl Langdon-Orr: Well that's great.

Mikey O'Connor: ...dispersion there.

Cheryl Langdon-Orr: What the hell?

Mikey O'Connor: Wow.

Cheryl Langdon-Orr: Holy moly.

Mikey O'Connor: Good, good, good; love it when they're - that's the precursor for a good conversation. Why don't we...

Cheryl Langdon-Orr: Holy moly, yeah.

Mikey O'Connor: ...pause and have a conversation about that. I'll switch over and start taking me some notes here so that we've got...

Cheryl Langdon-Orr: Wow.

Mikey O'Connor: ...that. Copy the rest of these in too. Getting the hang of this tool. Nice tool; I like it. And it's free so anybody who wants to use this tool can.

Why don't we just sort of run through the folks who voted who want to speak and just tell us why you voted the way you did. Can get a sense of whether we need to change the wording or what. Again don't be shy. Oh come on. There we go. Go ahead Jacques.

Jacques Latour: Hey, so I guess I took it from the perspective of being in Canada, right?

Mikey O'Connor: Yeah.

Jacques Latour: And the impact of the Canadian government doing something is less likely than other countries.

Mikey O'Connor: Oh I don't think that that's the right interpretation...

((Crosstalk))

Mikey O'Connor: ...of what we're about. I think that you need to put it in the context of - you know, I think the best example of this is still the SOPA debate in the US or some of the debates in the EU where a government not necessarily your own government but a government takes an action that disrupts the DNS.

Jacques Latour: So if the US government decide to block some sites in the US...

((Crosstalk))

Mikey O'Connor: No...

Jacques Latour: ...small portion of the planet, right?

Mikey O'Connor: Yeah, but what the US government was getting ready to do - and many folks including some on this call - raised this hands. They were getting ready to break DNS SEC because what they were going to do is they were going to put essentially a man in the middle attack...

Jacques Latour: Yeah but not for...

Mikey O'Connor: ...on all DNS SEC stuff.

Jacques Latour: They're going to break DNS SEC for some domains not...

Mikey O'Connor: DotCom...

Jacques Latour: ...the entire dotCom...

Mikey O'Connor: Yeah.

Jacques Latour: ...not the entire dotNet or all of the dotDe or all of dotCa just specific sites that were infringing specific copyright rules...

Mikey O'Connor: No the problem wasn't with the blocking the problem with the requirement that ISPs monitor the traffic. And whenever they saw the traffic going to that blocked site change its destination. And as a result that to DNS SEC looks like a man in the middle attack.

And so it was essentially putting major ISPs like, you know, AT&T or Comcast in the position of having to inspect all the traffic. You know, I'm now floating pretty deep into waters that I can't really articulate so somebody who's smarter about this than me should say something.

But it wasn't the blocking provisions I don't think that were really the issue it was the mechanism by which the blocking was going to be enforced that was the problem. Greg or Jim or somebody with a brain about this can you help me out? I'm floundering here but I think that's the key issue. Nobody is...

Greg Aaron: It seems like we're quickly getting into the realm of geopolitics. And the probability of one of the governments - and let's just arbitrarily say one of the

top 10 extensions by number of domains in that zone - the stability, the rationality, for lack of a better word, of those governments and their ability to intercede in the operations of DNS. And it's really hard to reconcile all of those factors it seems.

Mikey O'Connor: I think that's probably right. But...

Greg Aaron: It seems like depending on what we're focusing on each of us as an individual I think that's what's causing the disparity is that we're looking at it from perhaps one or two or three different factors but not necessarily all of us looking at all factors in the same way. And just to comment on what might explain the disparity of our ranking.

Mikey O'Connor: Yeah I think that's right. I have been lax in taking notes so I need to run back and capture Jacques's point too. Get this one finished.

Greg Aaron: So let me ask this: Do we feel - and specifically again using the arbitrary assignment of the top 10 - extensions by number of domains - and we look at the fact that some of those are gTLDs and some of those are country code extensions. Does a particular government have the ability to intercede in such a way to affect the gTLD or one of the, you know, their own ccTLD might be the first question to ask.

Do they have the ability? If they have the ability then we can say well okay what's the probability of them actually doing that? And then to one of the other member's comments okay so if the US government does something within the US does it really affect somebody in Canada?

So, you know, to your point, Mikey, it might depending on the implementation.

Mikey O'Connor: Okay, Jacques, you're back in the queue; go ahead. We've got some stuff going on in the chat but Jacques...

((Crosstalk))

Jacques Latour: Oh I forgot to lower my hand.

Mikey O'Connor: Oh okay. So going to the chat Bart is saying maybe ACTA is a better example. This is still on the political agenda and dealt with in a nontransparent manner. Rosella agrees with that. Greg is commenting that a government can affect the Internet in the way in - in ways that are outside of their ccTLDs, for example the dotUS. Cheryl is in agreement there.

One of the problems with the SOPA bill is it would have falsified DNS responses. Yeah, that was what I was stumbling along trying to say. And now James Galvin who actually knows what he's talking about can go ahead.

James Galvin: So this is Jim. I don't know that I necessarily know what I'm talking about but I did want to ask a question. I think one of the things that concerns me in this discussion has actually concerned me a few times along the way here is the scope of the question that we're asking because even in this case this comes up again.

You know, certainly a nation state - a country can decide to do something that would disrupt a zone but the question I have is are we talking about them disrupting the zone for the rest of the Internet or disrupting the zone within their sovereign perimeter if you will?

Mikey O'Connor: I think that we get to do that several times. In this particular pair what we're talking about is a nation state doing an action that has these consequences to a major zone file as opposed to...

James Galvin: So to a major - when you say to a major zone file you mean to that zone file in such a way that it affects the Internet as opposed to within the sovereign perimeter?

Cheryl Langdon-Orr: Correct.

Mikey O'Connor: Correct.

Greg Aaron: Yeah, that's a big difference.

Mikey O'Connor: Yeah. And I think that that's what this pair is saying...

Cheryl Langdon-Orr: Yes.

Mikey O'Connor: ...when we evaluate it. And I think that speaks to Jacques's point as well which is...

James Galvin: Yeah, because, you know, now that I rethink this a little bit, you know, I'm inclined to think that no they can't do something - it'd be very challenging, to say the least, I can't even think of an obvious thing they could do. I don't know if anyone else has something in mind where they could affect the rest of the Internet.

You know, they could certainly affect within their sovereign perimeter but no example comes to my mind as to what they could do that would affect the rest of the Internet.

Mikey O'Connor: That I think is exactly...

((Crosstalk))

Mikey O'Connor: ...what we're voting on is, you know, can we - have we ever seen this happen where one of the major zone files was disrupted by an action of a government.

James Galvin: Right now Greg is typing in the chat room here that he can think of some ways. You know, he mentions this business of universal resolvability but still

from my point of view that only affects within the sovereign perimeter. What could some nation state do to dotCom that would affect the rest of the Internet?

Mikey O'Connor: Greg, are you audio-impaired or can you jump in on the conversation here? Keeping up with this typing may be tricky.

Greg Aaron: Well what if dotUS - what if the US government and dotUS decided to fragment from the tree and splintered a root.

James Galvin: So? I mean, I'm not sure what you mean by splintered the root but suppose they decided to separate dotUS from the root; is that what you're saying?

Greg Aaron: That's right and say we're going to maintain our own tree - our own DNS and it's not going to be integrated with what we traditionally know as - like what China has done effectively, right? They splintered the root.

So I don't know specifically the ICANN regulations whether that would even be allowed. But what if we decided to say we're going to go play in our own sandbox.

James Galvin: Right but that doesn't affect the rest of the Internet is the point. It only affects...

((Crosstalk))

James Galvin: ...within their sovereign perimeter.

Greg Aaron: ...but - well the sovereign perimeter being the TLD space or the geopolitical boundary that - the physical geography, right, in the US borders or is it access to the dotUS domain, right? Subtle difference but technically different.

Mikey O'Connor: And again on this particular question, you know, I think...

Greg Aaron: Well, Mikey, I think you were really close to the ah-ha moment which is if we narrowly define or redefine this or re-articulate the meaning of this particular question which is can a sovereign affect the actual zone?

Mikey O'Connor: Right.

Greg Aaron: Not the end user experience in terms of, you know, ISPs intervening and the like. But can they actually affect the zone?

Mikey O'Connor: Right.

((Crosstalk))

Mikey O'Connor: Because we're going to get to the one that the - that SOPA did when we evaluate this pair I think. Because I think...

Greg Aaron: So if we - right. If we parse that out...

((Crosstalk))

Greg Aaron: ...narrowly define it that - it might be easier for us to vote...

Mikey O'Connor: Right...

Greg Aaron: ...and we might arrive at a consensus.

Mikey O'Connor: Yeah, I think on this one the narrow - the narrowly defining thing is helping us so I'm starting to see the value of the pair wise. And so it's for this pair that we're voting not all conceivable cases because presumably these other cases that we're going to take a look at, you know, will have a chance to weigh in on those as well.

And then one of the nice things is that at the end we can say okay well there are a bunch of them that don't have much of a score because they're either not going to have much of an affect or they're very, very unlikely but we're probably going to unearth one or two that would have a huge affect and are reasonably likely. And those are the ones that we'll allow to graduate to the next stage.

Okay I've got a bunch of hand - oh Olivier hasn't had a chance to talk. Go ahead, Olivier. Well you may be muted.

Olivier Crépin-LeBlond: Thank you, Mikey. It's Olivier for the transcript. Can you hear me?

Mikey O'Connor: Yeah.

Olivier Crépin-LeBlond: Oh okay thank you. There's a small delay. Just a wild question - wild guess here. If we take the example of dotNet because root servers dotNet, gTLD servers dotNet if dotNet gets shut down for whatever reason it is is that not likely to affect the whole Internet?

Mikey O'Connor: Right I think that that's the core point of this particular discussion is that we're evaluating a pretty narrow case right now that we tend to agree would have a fairly high impact or fairly high range of effects. In fact we may want to redo that vote as well because I think we now understand what we were voting for better.

Because I think that if a government accidentally did something that shut down dotCom we'd tend to agree that that was a pretty dramatic impact.

James Galvin: And so this is Jim again. Though there are two parts of this again. I think the point that I was trying to get to is I don't see how someone could do that.

Mikey O'Connor: Right. And that's why...

James Galvin: You know...

Mikey O'Connor: ...I think it's important to record both votes is to say well it would have a big impact but pretty unlikely or, you know...

James Galvin: Okay.

Mikey O'Connor: ...or pretty relevant. So, you know, that's the value in having both of these votes I think is to be able to say exactly that is that, you know, if somehow or another somebody could do it it would be a dramatic impact.

And the nice thing about recording this this way is that, you know, if we said just to put votes in your minds if we said this one has a very large impact; it's a 10. And right now it's possible but we can't think of how.

And then in a year - so jump back to Cheryl's point - a government does something that accomplishes that the sort of ongoing tenders of this analysis could plug that new value into that relevance answer and quickly find out the impact on the risk. So it's essentially a way to create a tool that could very quickly respond to changes in the risk landscape.

And so if I were king and putting votes into your mouths I would probably give this one a 10 for range of effects and I'd probably give it a 1 to 3 for the relevance because of the point you're making, Jim. It's kind of a stretch to imagine how they could do it.

But let's go ahead and - let's revote both of these. So, Nathalie, why don't you go ahead and - I hate to throw everybody's vote away but I think we've had a pretty good clarifying discussion. And so let's vote. We'll go back to range of effects first.

And again the question is ignoring whether this is conceivable or not what would the effect be? What would the range of effect be if a government did

something that shut down Com, Net, UK, De, you know, one of the major zones? Go ahead and collect those votes.

James Galvin: And, Mikey, I just want to point out that we're at the top of the hour here and...

Mikey O'Connor: Oh thank you, sir. Thank you.

James Galvin: ...I know that I have a hard stop here.

Mikey O'Connor: Yeah, thank you very much. We'll collect these and call it a day and we'll do the schedule later. The big schedule announcement is while you're finishing up your voting is that our meetings will once again concentrate on Thursday. They'll start early in the morning with the SSRRT Group and range all the way to our meeting which is in the middle of the day on Thursday.

And I think it wraps up at 1330 in the afternoon is my hazy memory. And we'll go into detail on that. We're up to nine votes. It's the top of the hour and three seconds so we'll let you all go. Have a great week. We'll see you next Thursday.

James Galvin: Mikey?

Mikey O'Connor: Yes, sir?

James Galvin: Just want to point out Greg's comment about an agenda item for next meeting in the chat room. Wanted to make sure you didn't miss that.

Mikey O'Connor: Oh thank you, sir. I will add that to the notes. Anything else? Any last minute pearls like that one that I'm missing because I'm scrambling because I forgot to watch the clock again? Okay we'll call it a day. Thanks all. See you in a week.

Cheryl Langdon-Orr: Bye.

James Galvin: Bye.

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

END