Transcript
DNS Security and Stability Analysis Working Group (DSSA WG)
08 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 08 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-20111208-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)

ccNSO Members
• Takayasu Matsuura, .jp
• Jacques Latour, .ca
• Joerg Schweiger.de (co chair)

NRO Members
• Mark Kosters (co chair) (NRO)

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

SSAC Members

ICANN Staff:
Bart Bosinkel
Glen de St Gery
Julie Hedlund
Nathalie Peregrine

Apologies:
Don Blumenthal – (RySG)
Luis Diego Espinoza,.cr
Patrick Jones

Coordinator: Hello, excuse me, this is the operator. This conference call is now being recorded. If you have any objections you may disconnect at this time. Please go ahead, your lines are now open.

Nathalie Peregrine: Thank you, (Louise). Good morning, good afternoon, good evening, this is (Odessa) call on the 8th of December, 2011. On the call today we have Rosella Mattioli, Takayasu Matsuura, Greg Aaron, Rafik Dammak, Cheryl Langdon-Orr, Mikey O'Connor, Olivier Crepin-LeBlond, Joerg Schweiger, Jacques Latour.

From staff we have Julie Hedlund, Glen DeSaintgery, and myself Nathalie Peregrine, and we have apologies from Patrick Jones, Luis Diego Espinoza, Don Blumenthal.

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

Mikey O'Conner: Thanks Nathalie, and we also have Mark Kosters on the call. He's coming in through Adobe. Mark, if you want you can use the mic on your speaker - or the microphone on your computer and join us that way if it turns out to be useful.

Welcome everybody, this is the standard moment of silence where we check and see if any changes to people's statements of interest. Okay, this is also a consensus call and so I'm going to get right to it, little summary document that I'll just breeze through.

But this'll be the call where we tentatively agreed that this 800-30 methodology was at least good enough for what we're doing, on the last call.

And so we'll just take a brief moment to sort of hit the high spots of the methodology and then try to arrive at final consensus and then get onto the work, which is pretty exciting.

So I just extracted the pictures from the methodology and thought I would just flip them up on the screen for you in the Adobe room. Basically one of the things that's quite nice about this methodology is that it gets us to a sort of a shared terminology, along with a shared approach to the work.

So this chart, the first time I saw it, confused me because this is the flow of threats and attacks but it's not the flow of the work that we're going to do, and that got me goofed up.

So working from left to right there are sort of predisposing conditions and controls that organizations have put in place and vulnerabilities that organizations have. And a threat source takes advantage of those, slightly to the right, and a threat source has capability intent and targeting.

And there are actually two kinds of threat sources. This particular picture is for adversary threats, but there's another that's non-adversarial that's sort of accidental type threats.

And then an adversary could initiate a threat event, and so one of the things that we need to evaluate during our analysis is the likelihood that they're going to do that.

Then there's the actual threat event. Then there's a result from that event, and we have to evaluate the likelihood of those results, and then their impacts, when we blend all that together we wind up essentially an organizational risk.

So that's the flow of the attacks and the threats and so on, but that's not the flow of the work. The work comes in a different order. One of the things that

this methodology does is start at a very high level, an organizational level and then the organization develops a strategy. Out of that strategy comes the methodology and then out of the methodology comes the process.

And we sort of did that in a slightly different order but a lot of the work that we did fits quite nicely into this process and maps in pretty well, and I'll show you a bit of that.

We went through a lot of this in a great deal of detail on the last call. So unless somebody really wants a repeat of the 50 minute Mikey lecture from last time I'm going to skip most of that. But if some of you are new to this and still uncomfortable with it, feel free to raise your hand and we'll do a little detour into that.

One of the concepts that we talked quite a bit about last time was this three tier approach. And, in general, I think that it's safe to say that we are at the Tier 1 level, the very broad level, with this analysis. But we've got an opportunity to maybe take one type of threat event, which would be a DDOS attack all the way down to Tier 3, the very detailed level, or at least Tier 2.

Just to get sort of a blend of the very high level stuff that we're mostly going to produce, but at least one and maybe one or two much more detailed ones.

And so then the final picture that I liked out of the methodology is this one which is the actual flow of the work. And we did a - by accident - a fabulous job of preparing for this risk assessment, that's the first task. And as soon as we bless this methodology, presuming that we do today, we'll dive right into that first task which is, "Identify threat sources and events."

And we've done quite a bit of the spade work for that first task already, and I've attempted to map it into the methodology because I decided that it mapped pretty well and you probably wouldn't want to sit through the process. It took me a couple hours to do that.

So anyway, that's the - at a very high level - sort of five minute overview of the methodology. And again, we had a preliminary consensus on last week's call. We've also talked about this a fair amount in the leadership group and there's (consensus) there as well.

So this is sort of the last and final formal consensus call on this, and unless there's objection we'll go ahead and consider this one of our consensus decisions and I'll push it off to the wiki. So last and final call, any thoughts?

(Clock) is in. Okay, I think this was actually quite a worthwhile adventure. We got through it pretty fast. It only took us three or four weeks to get this decided, and I think we've done a very good thing for the community by taking a moment in our work to pick this because I think this will build a good foundation for subsequent times through it.

One of the things that the methodology sort of presumes is that we'll not - we won't be the first and only time through this. We'll be the first and then periodically this will be updated and refined and challenged and so on.

Okay, well let me show you where I'm at here. What have I just done for the screen to go black? There we go. I want to show you how I mapped our work into methodology. Is that big enough for people to be able to see? A little small. Let me just go up one notch.

What you see on the right side - or on the left side, is the whole methodology. So, all of these boxes are those major tasks that you saw on that prior slide. And what I've done is for this task what we're working on - I haven't done it for the rest of these, I promise I will but for the one that we're working on right now I've taken the methodology and I've expanded it to - I need more coffee this morning.

There. There's - in the methodology is - there's a bunch of get ready work, and then there's the actual work of the task. And I've built a little Excel spreadsheet of these that we'll get to in a minute. But I want to show you in the methodology they provide a preexisting taxonomy for us to start with, and what I've done is I've mapped our work into the taxonomy that they provide.

And I just want to step through what I did to make sure that I did this right. What I did is I took our threats work and I basically just dragged the pieces. So the stuff in green on the screen is the words and phrases from our threats document, and I've tried to drop it into the taxonomy of the - that the methodology provides.

And for the most part the threats that we identified that were adversarial are not individual threats. They're not a single outsider or insider or privileged person, they're groups that are trying to do bad things.

Remember, this is not threats that we're talking about this is threat sources, this is where the threat comes from. And so in our prior work we kind of commingle those two things. And so, for example, when we talk about government seizure of a registry operator, that's really a threat event that's initiated by a nation-state, and so the threat source is a nation-state.

And I just - because we had identified some threat events I just tacked them in there. But you'll see on the spreadsheet that those are just listed as examples, they're not - we're not quite to the threat event stage of the work yet.

So, that's the mapping of the adversarial threats, at least a first try. Then we have accidental threats, and that's where we do see some privileged user kinds of threat events. You know, a privileged user could be a threat source if they completely goofed up the configuration of a key server or system. And so privileged users can be threat sources but they're not, for the most part, adversarial, they're accidental threat sources.

We also had our discussion on a business failure. You know, and in Greg's honor I have to note that Greg, we need to circle back to this one still. I know that you disagree with us in thinking that this is a threat source, but we had a couple of conversations where the ALAC was pretty keen on the idea of including business failure as part of our work.

Oh, Mark is saying he lost audio. Has anyone else? Mikey says thought the audio, "Has anybody else lost audio?" Let me...

Greg Aaron: No, I can hear you.

Mikey O'Conner: Jacques is saying he's okay. It sounds like - Mark, it sounds - okay, Mark. Let Mark go off and solve that one on his own.

Greg Aaron: Mikey, can you hear me?

Mikey O'Connor: Yes, I can.

Greg Aaron: Okay.

Mikey O'Connor: Yes, it's all good. Did you want to say something? Now I can't.

Greg Aaron: I don't think I ever - were you saying that I had not wanted business failure to be in there?

Mikey O'Connor: Yes.

Greg Aaron: Actually, I don't recall seeing...

Mikey O'Connor: Oh, good. Well, we can circle back to this one. This was one we put back under discussion. For awhile we had it out of scope and I think - well, I don't want to get sidetracked on that, but anyway, all of these are still under

discussion, especially business failures. So we can circle back to those.

And then this last one, nation-states appears twice. Nation-states can do things on purpose, activism, etcetera. They can also do things by accident.

And I decided that the legislative actions that had unintended consequences, that could break the DNS fell in the accidental category rather than the adversarial, and so that's another choice that I made in this mapping.

And all of this is on the table, I just want to step you through it real quick so that we can then move on to the next chunk. In the methodology, then they also have something that they call structural.

And we had a bunch of these in our work as well where we talked about key equipment failures, environmental failures, and you know, we didn't identify many in this environmental category.

And so I didn't carry any of those forward. But what we did come up with was a pretty good list of things that have to do with storage and processing. We had some communications ones. And then these two, we had in threats, I - because of the way I was doing this, I was dragging every single one of our threats into this spreadsheet

What I did is I dragged those in and then highlighted them and said, "I really think that's an impact rather than an actual threat event." But we can circle back to that one and decide.

And then the other kinds of threat event sources that we did come up with were some of the sort of software infrastructure components. And you'll see that I collapsed these a fair amount in the spreadsheet. There wasn't a real strong appetite amongst the group to go into a whole lot of detail on some of this stuff.

So I kind of collapsed that a bit when I did the list for the spreadsheet. Then finally, the methodology has a taxonomy of environmental and this is mostly the disaster sorts of things. We did have a pretty lively discussion, especially about floods, hurricanes, earthquakes and then infrastructure failures.

So that's what I mean about the work that we did before fits pretty well into the methodology. And if you'll bear with me for just a minute, I want to switch from this to the spreadsheet that I built this week to show you what I've come up with. This is going to show up, shows up fine. So now I'll look at it. That's quite small. Let me make that bigger, little easier to read.

Can people read that okay? Let me just - one notch larger. There, that's easier, I think. But what I did is I built two tables and you'll see that this workbook, I think, is going to wind up being our primary deliverable.

Because my plan is that I will just build a tab for each of the tables that are called out in the methodology. And at the end, we'll just have this spreadsheet with a whole bunch of tabs across the bottom that will be the - basically the work that we've done.

And then from that we'll write this in English. So let me just give you a tour and I will post this every week to the list and to the wiki so that people can see, as we work our way through this, you know, where we're at and the decisions that we've made.

So in the - this is the adversarial threats page and basically all of the ones that we identified boiled down to five: People acting as individuals or in small groups coming at us. Terrorist groups and we could even combine these. We talked a little bit about alternate DNS root operators as a malicious, adversarial threat, and then nation-states in their adversarial role. And I gave those examples just to sort of consolidate all of the work that we'd already done.

So then what you'll see is that there's a - essentially a rating scale for each of these three things: Capability, Intent and Targeting.

And on the spreadsheet what I've done is I've summarized - well, no, I haven't even summarized these. The scales are listed directly below. So in terms of Capability, if we put a 10 in there, we're saying that this threat source is very sophisticated, has lots of resources, can generate lots of continuous, successful, coordinated attacks.

And then the range in terms of capability is all the way down to very limited resources and opportunities. And so that's the Capability scale and if we type in a number, we get pretty colors.

So, you know, if we put a 1 in we get, you know, a little worrisome thing. But if we put a 10 in, we get bright red, and so this is the standard sort of color coded deal.

The same sort of thing goes on with Intent. Again, there's a scale. The intent is quite worrisome if the adversary is trying to really basically destroy the DNS. And oops, it's less worrisome if they're down at the bottom of the scale and, oh, then there are ones in the middle.

And then finally there's the Targeting one and again, there's a scale, it's coming from the methodology which is, you know, very sophisticated targeting, if they're coming in with reconnaissance and attacks to the target are coming persistently at an organization all the way down to not such worrisome targeting. And this is the three scales that the methodology has us evaluate the threat sources on.

Want to take a moment partly because I don't want this to become another 50-minute Mikey lecture but partly because I've got a question for the group. And that is there's two ways we could approach this; I could send this out and

we could all fill this in and then send them back. And we could evaluate those results, you know, essentially a week later.

Or we could just do this on the phone on calls; we could just basically step through each of these cells and say all right for rogue elements what do we think their capability is? What do we think their intent is? And what do we think they're targeting. And we could just fill it out on the phone without doing the statistical exercise in between.

And I'm quite open to your thoughts on this; I don't know that I really care. And so I'd be curious to see what people think whether it's worth going out and doing a statistical exercise.

I think one of the things that's not so much a problem for this one but may be a problem later on is when we get down into threat events and we have spreadsheets going out and getting filled out by individuals we may start to run into the problem with sensitive or confidential information where people are kind of on record. And, you know, that may become an issue. But this one I don't think is that way.

Rosella raises a really good...

((Crosstalk))

Mikey O'Connor: ...question in the chat which is will we have the tables in advance? And the answer is as of today, you know, and today and from now on yes. What will happen is I'll build these tables and push them out to the list. This time there wasn't time to do that and I needed to sort of introduce it.

But in general, yeah, we'll always have these tables in advance. And so, you know, we can do this either way. Jacque, go ahead.

Jacques Latour: Yeah, Jacques here. I think we should, for everyone that can, try to fill in the spreadsheet on their own, get a feel for the impact of putting different values for different thing. And then once everybody did it on their own then I think we should do it on the phone and then - it's - so everybody gets a chance to do it before; they get to learn the tool, play with it and understand it. And then if we do it together we have a better chance of getting consensus...

Mikey O'Connor: Oh I like that. Yeah. I like that a lot. So not actually analyze the stuff that people have done, just do it, have it ready for the call and then - or are you saying bring the results back and combine the results before the call as well?

Jacques Latour: No but - no we don't use - like my results are my results...

Mikey O'Connor: Yeah, okay.

Jacques Latour: Because they're going to be biased toward like a ccTLD.

Mikey O'Connor: Yeah.

Jacques Latour: And then I think a discussion is going to come out that people have different perspective.

Mikey O'Connor: And then during that discussion we try and arrive at a shared answer.

Jacques Latour: Yeah.

Mikey O'Connor: Yeah, that's a great approach; I like that a lot. Any other thoughts on this? Because what I could do is, you know, this pair of tables is pretty well done. And so I could send this out right after the call and people could spend the week then - as Rosella is saying so then we can think about it before the call and discuss it maybe even online on the list and then jump in on the call the following, you know, next - in this case next week and try and fill out the stuff together.

I'm quite taken with that because I think that if we do it that way and we sort of set ourselves a pace of a table or two a week we could be very close to a final result by Costa Rica which is quite exciting to me. I think that would be a pretty amazing piece of work by the group and would give us a lot to talk about with folks at the Costa Rica meeting.

Trying to decipher Cheryl's comment. Happy to do prep then run as a group. I think next week yes. Okay so let me interpret that; this is a creative interpretive reading. I think that what Cheryl is saying is she's happy to do it, prepare then do the session as a group. And I think that might be group-think and - the following week and then yes. So, Cheryl, if I misinterpreted feel free to correct me.

And Rosella is chiming in saying that she likes this methodology and approach. Good, I'm glad of that. The methodology makes a lot more sense as we get down to the nitty gritty of these tables. And so I am feeling much more comfortable with the methodology as well.

Okay well gosh that's kind of all I have. I think what we'll do is stop at this point today because I think the next step is I will turn right around and send this out to the list and let you all spend the week filling it out on your own. And then we'll just start right on this page next week and work our way through it and see how that approach works.

And see if - I think our goal for next week could be to try and fill out both this table and the next one. Let me show you the next one, it's slightly different. With adversarial threats we have this three-dimensional analysis that we need to do, how capable are they, what's their intent and what or who are they targeting.

In the case of an accidental threat source there's only one. Again, make this a little bit bigger. Because this is accidental the notion of capability, intent and

targeting doesn't make any sense. And instead what the methodology says is well what kind of effects does this sort of accident have, you know, how wide ranging are those effects. And again I've just posted the scale right underneath right there.

So a bad one would be one that has really broad effects and a not so bad one would be minimal. And the scale is 1-10. The - with the numbers. So when you type in here - you don't get to type words you only get to type numbers so again if you type 6 in there you get a little orangey deal. That's how that works.

Let me - since we're doing this for ourselves what happens - yeah and you can see the number. Yeah, all right so this will work fine for our approach of filing it out ourselves and then having conversations about it.

So with that I don't know, I guess I don't have any more material unless people have questions or would like to change these or - Rosella is saying is there a definition of geopolitical groups? I think it can overlap.

And Jacques got a good - let me answer Jacques question first because that's easier. One of the things in the methodology that they say is that when we are doing these analyses we ought to make up an identifier. And so I made those up. And so NATS stands for non adversarial threat source. And then I put - being a computer programmer I started them at 10 and went up by 10 so that if we wanted to insert one in the middle we could do that.

So that's where that one came from. And then in the other one it's adversarial threat sources. So that's all that is, it's just an identifier. That - I'm not exactly sure of how those are used but I have a suspicion that when we get into subsequent parts of the methodology that they may come in as a useful way to shorten and abbreviate and cross reference a thing. That's what I did.

In terms of geopolitical groups that's true. I think that one way we could consolidate this is to consolidate terrorist groups and geopolitical groups into one. I noticed that as well. Does anybody have strong feelings if I went ahead and did that if it's just one thing? So it would be geopolitical groups and then in parentheses by way of example I could say terrorist groups, activists, you know, global activist groups, something like that.

Okay Cheryl says fine, getting lots of typing so we'll take just a pause while the comments come in. Rosella is saying or we could state clearly the difference. And at first sight it's not clear. I think that's right, Rosella, I think there really is pretty substantial overlap and probably geo - terrorist groups is one of our terms, geopolitical groups came from the methodology. And I think that the - is the phrase that we might want to settle on.

Jörg, which one are you favoring? Jörg says heavily politically incorrect but nice for this purpose. Terrorist groups or geopolitical groups is - I didn't realize that either of those were incorrect.

Rosella is coming up with non-state actors.

Cheryl Langdon-Orr: Cheryl here, Mikey.

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

Cheryl Langdon-Orr: Cheryl for the transcript record. I think we will need to be politically correct eventually. So perhaps it would be worthwhile to try and establish some shared and agreed nomenclature now and just...

Mikey O'Connor: Yeah.

Cheryl Langdon-Orr: ...you know, as painful as that will be to perhaps use something wordy it will probably be in our best interest in the long run.

Mikey O'Connor: So what - which one - I was unaware of the incorrectness - is it geopolitical groups that's incorrect or terrorist groups that's incorrect?

Cheryl Langdon-Orr: That's probably going to - Cheryl again for the record. That's probably going to depend on who you ask. But my gut reaction is that the term terrorism is value-laden while geopolitical is less so because my freedom fighter is your terrorist.

Mikey O'Connor: Yeah, okay. So let me just fix that. We would just do it like that. And then maybe to sneak Rosella's words too. How about that? Does that work for people? Hearing that glorious silence of problemo, okay.

Good, all right. Anything else that people want to do to this table before I send it? Let's just look at this page for a second and see if there's anything else we want to change. And then I'll put up the other page. And I'm getting pretty much thumbs up on this page. Let me go to this one. That was a good refinement so we'll just take a moment.

For example one that we could combine is we could put those two together and just say hardware failures. Make this a little bit - that's a good idea. Let's see, where am I going to put that? An assumption column on this one. That's one quick...

Cheryl Langdon-Orr: Mumbling, Mikey.

Mikey O'Connor: Sorry. I have to do it once every call so just to keep you on your toes.

Cheryl Langdon-Orr: I know you do it just for me, thank you.

Mikey O'Connor: I do. You know, it's part of my goal since you're on the phone so late it's part of my goal to make you smile at least once on each call. All right so let's combine these. Say hardware failure - no I'm going to do this in assumptions in notes instead, rather than watch you suffer - let you suffer through me

struggling with this. I'll combine these two but I don't want to spend time - oh, Olivier, go ahead, sorry, I wasn't watching the Adobe room.

Olivier Crépin-LeBlond: Thank you very much, Mikey. It's Olivier for the record. In the adversarial threat sources we do not differentiate between insider threat sources and outsider threat sources, i.e. a rogue element inside a company actually working, being part of the - inside the (fruit) or a rogue element coming from outside and being totally unrelated to the organization. Should we make the differentiation between the two or not?

Mikey O'Connor: That's a terrific question. And I defer to people who know more than me. In our conversation we never described an insider doing that but it's certainly in the taxonomy that came with the methodology. So I defer to folks who've actually got experience with this as to whether insiders have ever been a threat source in case we certainly should and it's easy to do. Rosella is lobbying in favor of insiders.

Olivier Crépin-LeBlond: Mikey, it's Olivier. I think the statistics show that I wouldn’t say the majority but there is a very large chunk of hacking and sort of damage done to corporations from insiders, i.e. disgruntled employees or ex-disgruntled employee, etcetera, etcetera.

Mikey O'Connor: Right. Yeah. No - yeah all right. We're getting pretty much unanimous agreement so let me just...

Cheryl Langdon-Orr: So certainly - Cheryl here while Mikey is not mumbling; just filling in the dead air space I guess. But from our ccTLD perspective it's been insider risk at least here in Australia. And actually not the risk; the actual damage when we've had the need to de-register due to bad things happening it's been insiders have done it. And then other compounding areas have happened after but the (first) source has been insider.

Mikey O'Connor: Yeah, okay. Good, all right so I think I'll just duplicate it that way, have insiders and outsiders. Now do we have inside - notice that what I've done is I've put them both in the small group category. Do we have insiders that are actually acting as part of a larger organization?

Cheryl Langdon-Orr: A geopolitical group?

Mikey O'Connor: Or is it safe to call them, you know, rogue individuals or at least small groups like small groups is okay. If you, I mean, again what we can do is refine this after we've each had a chance to sort of go through it cell by cell and decide on that.

Okay the queue is clear. Let me go back to this one. Anything else on this list that leaps out at people that needs to be refined? This is really good refinement. I don't want to give it short shrift. All right well let's take this as version one. I'll send it out to the list. I'll make that combining work and send it out to the list, you know, within the next half hour or hour and - with a note sort of describing what to do. And then we'll pick it up at the next call.

If we've gotten through this whole thing by the end of next call we're about 1/5 of the way through the analysis and we will be really moving along at a terrific pace. So if it feels like we're going too fast after the next call don't feel bad about slowing things down because even if we took two or three weeks per table we would have a lot to talk about in Costa Rica.

((Crosstalk))

Mikey O'Connor: Pardon me, Cheryl, go ahead?

Cheryl Langdon-Orr: I think that's a good plan.

Mikey O'Connor: Yeah. Okay people thanks very much. That's it for me unless there's any other business. I'm seeing some typing. Oh thanks, Jacques. Always - I think

one of the things we don't do real well at ICANN is give each other strokes when they do a good job so it really does mean a lot to me to hear that this is going okay. Thank you.

Okay that's it. We'll see you in a week. And, Nathalie, I think we can end the recording and wrap this one up.

Nathalie Peregrine: All right thank you, Mikey. (Louise), could you please stop the recording. Thank you.

Coordinator: One moment please.

Cheryl Langdon-Orr: Oh this is excellent, thanks, Mikey. It really is...

END