Consultation-security-strategic-initiatives-08mar10-en.mp3
01:03:10
Transcribed 03/12/2010 LNC

Greg Rattray: I'm going to move into the two – there's two documents – one document is the Strategic Initiatives, this slide addresses the first portion of that document which tries to lay out a risk framework for the domain name system, you know, which precedes the actual content of what activities ought to occur in order to deal with these risks.

This paper also discusses the DNS-CERT; we also have a DNS-CERT business case which again Yurie is going to address in more detail.

So I am not going to go into, you know, detailed explanation of the risk analysis that's present in the Strategic Initiatives paper but to make the point – really I wanted to make the point that it's not just malicious activity but that there are other risks to the DNS that stem from technical vulnerabilities and organizational failure.

The point here being that there needs to be – for the domain name system – if it's going to be secure and resilient – structured risk analysis that's got community buy in.

The other thing, which, we had another symposium just last February on Security and Resiliency, is that we need to improve the metrics and measurement of what constitutes sufficiency in things like security and resiliency and DNS health.

So the next slide.

So Initiative One – there's a couple of slides here, I wanted to kind of go into some of the major capabilities posited as necessary in Initiative One. Again, if you read the document, it envisions a community based effort – actually suggests that there should be, you know, a group of experts that are conducting this set of activities outlined here that this would be supposed in a staffing way by ICANN. Again, that's open for comment.

That the activities that are necessary is to get an established risk framework. Get a baseline. Make sure there's community buy in to it. As well as identify what sort of key contingencies or scenarios, based on the key risks, are out there as a basis for some of the further activities including contingency planning and exercising.

That this should be a regular process. I suggest in the paper annually. That, you know, this annual process for ICANN, you know, whoever does it, would serve our security and resiliency planning, our operational planning, you know, this should be driven by risk analysis. An annual assessment would allow us to do that. I certainly believe other organizations could also feed off an annual DNS risk assessment.

The U.S. government for example and probably other governments and critical infrastructure protection organizations do risk assessments which include the domain name system on an ongoing basis.

The finally, well not finally, while we are still in the process of taking the root scaling study that was produced last summer and working through the implications, one of the clear things called for in the root scaling study was a root server information sharing system. We think this should be part of the initiative that being able to understand security and stability concerns at the root system level should be part of what gets instituted under this initiative.

Next slide.

And then further, again, the Affirmation of Commitments explicitly identifies contingency planning as something that ICANN is responsible for doing so that the initiative includes the notion of how do we do contingency planning. In my mind this links back to, you have to understand what your key risks and contingencies are based on scenarios. So that's how the paper lays out doing that is to identify those scenarios and conduct contingency planning based on those scenarios.

And then finally a mature, you know, system-wide program for dealing with risk would include actually exercising the contingency planning that you have. I mean, that's kind of the full cycle of proactive security at a big system level.

There are exercise activities that go on that involve the DNS now. There's been gTLD continuity exercises. Certainly each of the individual registries and registrars probably conduct exercises. The multinational cyber storm exercise involves the DNS, has historically, will again in its next iteration. All of these things should be part of a more general, you know, program for ensuring that we are exercising the right aspects of Domain Name System security and resiliency.

Again, the initiatives paper outlines mostly a staff based resource requirement at $2.1 million. So with that, I'm going to turn the briefing over to Yurie and allow her to cover the DNS-CERT initiative.

Yurie Ito: Thank you. Good afternoon. I will be describing the DNS-CERT.

So this is what I'm going to talk. Let's go to the next slide, please. Thank you.

So lesson learned – we have experienced the last couple of years those incidents as a community – Conficker and also we handled those particle level vulnerabilities – also Aberange (sp?), Botnet – there are large numbers of Botnets out there and you know, some of these are really largely impact to registration, DNS operators community.

So we walked through working with the community, we walked through all of this incidents. And experienced those responses and we got community voice and requests that they need a community mechanism, the systemic community mechanism to respond to those types of incidents as a community.

Next slide, please.

So hearing those voices, the Security team has started working with the community and developed this concept of DNS-CERT. And the mission of this DNS-CERT is ensure DNS operators and supporting organizations have a security coordination center with sufficient expertise and resources to enable timely and efficient response to threat to the security, stability and resiliency of the DNS.

Next slide, please.

We heard from 2009 DNS Security, Stability, and Resiliency Symposium – that symposium theme was to list all of the threats and risk to the DNS. And the participants of that symposium pointed out that the resource constraint operators are not reaching out to those technical networks or technical resources. So when they have experienced all of these incidents or facing against the threat, they don't, you know, have much support or technical network to reach out.

So we quickly did – we heard about that voice – we did some capacity analysis because we were aware that there are existing response efforts out there in the community. For example there are DNS-OARC, there's a Registry Internet Safety group, and also CERT community like FIRST and the regional CERT organizations and frameworks are out there.

I have excluded all of the private and selective groups from this list but they are, because they are private groups, and it's, you know, if you're looking for those informations, there are no information out there on the Internet. So I excluded all of those lists.

But if you are an operator or CERT community, you might be on those lists. So you might think that they are already existing those response community and framework or mailing lists out there.

But the thing is, if you analyze who is on the mailing list and who is working on there, these groups are the very key resource who they are developing the remediations are all there on this mailing list. But for those resource constrained operators are not really – these groups are really not outreach to those operators.

One of the reasons is really because most of them are – some of them are membership organizations – charged membership – and information are only within the members. Or some of the groups are really secret hand shaking society that if you don't have trust, face to face trust relationship, it is very hard to be vetted and getting into that community.

So next slide please.

So we found the gap there and disconnect the community there. So what we try to do is talking to those core response resources groups and did some capacity analysis, find the gaps, identified the gaps, and the DNS-CERT is trying really to leverage those existing efforts and try to avoid to exhaust those resources but those information to deliver to those resource constrained operators who are actually currently not accessing to those key resources.

So goals of this DNS-CERT operations is to provide the full time and global coordination mechanism or coordination function to the community. And bridge those key resources to the disconnected resource constrained operators.

Next slide please.

So these are the stakeholders by role. If you can take a look at that, the DNS-CERT key stakeholders are, of course, the DNS operators, registries, registrars, root operators and also especially the resource constrained operators as well, and the registrants. And also if they are not listed in this chart, but the cyber-security response expertise, cyber-security community, they are also key stakeholders. And also the response is not only the technical but it could be the government level or policy level or law enforcement level. So they are all stakeholders as well.

Next slide please.

So we developed this concept and it's a very key is to get the needs from those key constituents. So we are talking and having a dialogue with the CERT community and find out what we can do. Not every CERT is specialized for DNS so we hope the needs of, if there's a DNS specialized CERT out there, when they experience incident or threat against DNS, they can reach out the information from the DNS-CERT.

And also we are having the dialog with the geographic reach. So we're talking with the regional TLD association and talking with them and asking their needs. So we talked with Africa network operators group, AfriTLD, we gave a briefing at the center and also APTLD, we're planning to do so at the MENOG as well. Trying to do outreach to those geographic community and find out the needs.

So it's very important for us to keep focus on constituency needs. And right now it's a concept, developing the concept. If we keep continuing community dialogue, and identify the needs and get the support, we are going to now discussing about with the community to implementation phase. So how to implement – this is a rough number of the funding is here.

We calculated this number really to see the similar size and similar service level of the CERT. And we calculated this number. But of course, how to implement it, how to be, you know, funding and formation, all of these things are going to be after the service level discussion and the concept being discussed and supported by the community, we'll move on to this discussion after that.

So with that, I will give this back to you.

Greg Rattray: Thanks Yurie.

So, the way forward is pretty straightforward. We are at the stage clearly of seeking additional community feedback. This, you know, session here is a core portion of that. We know we have some significant remote participation so we'll get into some of that right now.

And again, it's very clear that, you know, if there's support for these sorts of capabilities, the next stage will be to address, you know, options for how do you organize to create these sorts of capabilities and funding.

So, you know, I think that's the next major challenge in pushing these initiatives forward.

So with that I think that we'll just stop. Again I want, Liz I want to ask you a question. Are we already starting to get questions queued up?

Okay, so clarified the one question. So we'll start with questions here. Liz please raise your hand or interject if we start to see questions from the remote participation.

You should use microphones because the session is being recorded and transcribed. And if it's acceptable to everybody I think I'll sit down.

Unknown male: Actually this first idea of DNS-CERT was proposed at the last meeting in Seoul. What's the progress from that time?

Greg Rattray: I'll take that.

So the notion that, you know, a DNS-CERT might be one of the ways to respond to the growing kind of dialogue about need for collaborative response, response to Conficker worm, was discussed you know, in different forums, kind of as a notion. At that point, we didn't have the support in the strategic plan. You know, we had not formalized those initiatives. So the progress between Seoul and this meeting is actually to write a DNS-CERT business case, you know, it's now validated as some of the strategic plan and now to engage the community in a structured fashion about whether this is a right-minded notion, is the scale of activity, you know, described the right scale of activity and to begin to get feedback on that concept.

Peter?

Peter Van Roste: Thank you Greg and Yurie. My name is Peter Van Roste, General Manager for CENTR, the European Association of ccTLDs.

I had a couple of questions and comments which do not affect; I must say the principle of this discussion, because I think it's a very relevant one to have.

And I suggest I just go through them and you can take whatever you want from that.

You mentioned that there were plenty of community calls that were at the basis of this DNS-CERT ID and for us it would be very useful to understand where those originated from. Because the ccTLD community has a rich history of helping out its members and if some of the members of that community would claim that they do not have access to that relevant information then it's very important for us to figure out how we can improve that.

And also because, from what I've heard both within the CCNSO, the CENTR community and APTLD, the Asian community, of which I attended a meeting last week, that claim did not originate from those corners. So that would be very helpful in particular because it would also help within understanding what the exact nature of their needs is.

And from what we see, and based on the information that you've shared with us, I think that we identified a real problem, that is, during the Conficker attacks there was an issue with communication but it seems that issue can be solved in a much cheaper way than a $4 million dollar organization.

There are the obvious overlaps with the existing processes which you point out but by just pointing them out we still think they are still relevant and they're still there so we need to figure out how we could solve that.

And then it's also unclear on how it fits into the overall budget. From what I understand, it's not included in the overall budget at the moment. The business plan itself mentions that ICANN would be prepared to basically kick start it. But I always find it, running an organization myself; I find it a very tricky process of starting something and then looking for funding. Mainly because we have seen that process on a number of other occasions such as the trainings for instance for ccTLDs on a technical level.

I think it's very important that during this consultation, the right question is asked. And that question should be, "If you think you'd benefit from a DNS-CERT, would you be willing to pay for it?" Because obviously everybody is always interested in free candy.

So these are my basic points and maybe we can discuss this.

Greg Rattray: Peter, I'll leave the last one as kind of an assertion which I agree with that it's a fair question to talk to people during this process about their willing to fund. I want to try and remember at least a few of the previous ones. I'm also going to let Yurie give her perceptions.

One of the main drivers was this symposium last year where it was clearly identified and Conficker had just emerged at that point, you know, the notion of the need for stronger collaborative response capabilities and some of the Conficker after action reporting that has gone on in the Conficker Working Group you know, has validated the same notion.

We did not get any specific requests from a TLD association related to this. Though again, as Yurie pointed out, we've had a number of discussions when them and have received you know, feedback from some that, you know, exploring the notion of this capability would be very useful.

Peter, I'm starting to lose, what was the second, that was the first question, what was the second question?

Peter Van Roste: It was probably more comments. That we identified a real problem but that from my perspective and a couple of my members, because obviously this is not just my opinion, we are probably shooting at a mosquito with a cannonball.

Greg Rattray: Which, you know, I think we'll end up stressing this point a lot in the discussion, is that those who are well connected, which I think a lot of the CENTR members are with strong security resources, probably do perceive less of a need for such an organization. But we have received feedback from operators in Africa, you know, the southeast Asian nations, where their, you know, understanding of the issues, situational awareness, their ability to get information in situations like Conficker or the emergence of domain hijacking, is much more limited and therefore the utility of an organization that was explicitly focused on sharing with them, might be higher. But that's, you know, to be validated by those, you know, people in those seats, and you know, I think an important of what will come out of the consultation is that perceived need actually there.

But I know Peter I also haven't addressed your full list of questions, so what was the, can you hit anything else that we haven't discussed?

Peter Van Roste: Well, I think you hit there the most relevant part of the whole discussion from our perspective, pointing to the operators in Southeast Asia. I mean, I've talked to them and I couldn't find them. I'm sure that those that are well connected as you refer to them, would be very happy to shepherd them into that community, that closed community with the secret handshake.

I think it's a very important task of the ccTLD community that they take care of the other cc's that are apparently not well connected. So I'd really appreciate, and obviously you can do this afterwards not in this public forum, but if you could help me in finding those people that feel that they're not connected.

Greg Rattray: Understood.

Yurie, do you have any other perspective from your interactions? And then I'm going to give Liz a remote…OK.

Liz is there somebody remotely that we should? And then we'll get around the room.

Liz: So there are two questions in the chat. One from Pat Cain and one from Chuck Gomes. So you have two in the queue.

The first is Pat's, "Greg, what are your current expectations for the exercise program of registries and registrars?"

Greg Rattray: So you know, really I have no well-formed expectations. I think it needs to build on the gTLD community has been involved in a continuity exercise program. I think the best way to define the requirements for an exercise program is first to go over with everybody what exercises already exist. Again, I would imagine so of the organizations, probably including Pat's, have some pretty robust internal programs. I think that for registries and registrars the question is, "What sorts of coordinated responses they need to take and you know, how does one structure an exercise program that allows them to practice working together?" Pat's organization and Pat as an individual specifically, VeriSign's leading a distributed denial of service mitigation cooperative, collaborative effort. You know, that's the type of thing that I think would involve exercise sorts of activities because it involves multiple organizations simultaneously.

Liz: So the second question from the chat from Chuck Gomes is, "When we will be able to see the cost breakout for the $2.1 million dollars? Where did that amount come from? Whoops, the chat moves. "It is impossible to evaluate the validity of the amount without much more detail?

Greg Rattray: So we can, you know, detail the constituent portions of that $2.1. I hadn't actually planned when we would, you know, publicly post the deeper analysis of the costs listed there. We probably should do that, you know, especially if there's going to be appropriate calls for a more detailed analysis of the funding requirements. So committing to do that, I don't want to commit at this time to the specific, you know, timing of that but, you know, weeks not months.

So I know Wendy had her hand up. We probably need to do some sort of queuing process. So I'm going to go Wendy, then to the left and then, yeah, to her left and then back around this way.

Wendy: Thanks. My question is about the scope of the activity on the first risk analysis and particularly in malicious activity risks. Where you, at least in the paper, seem to sort of pull together two what seem to me very distinct sorts of risks, the attacks against the DNS itself and attacks that exploit name resolution or registration systems. And my concern is that while it's relatively easy to identify an attack against the DNS, one person's malicious activity using the DNS can be another person's useful exploitation of unexpected properties of the DNS. And so, how do you plan to cabin the scope so that malicious doesn't expand too broadly?

Greg Rattray: As probably many in this room know, I completely concur with the notion that the first category is much more easily defined and that the second category is a work in progress for ICANN in terms of, you know, what constitutes the right boundary and one would, I think probably accept the notion of a large, you know, multi-million computer botnet utilizing the Domain Name System as a systemic risk to Internet security writ large and, you know, to the Domain Name System itself. You know, I think you're right Wendy, there's a lower end of activity which is much grayer or, you know, much more questionable whether it's malicious in intent or not. You know, part of both efforts, you know, what the CERT response to in addition to what's just considered a risk, will require, you know, some boundary setting on, you know, the lower end of that.

I think, in my mind, we really want to keep the boundary pretty high. The notion that we're going to do risk analysis, you know, for every type of bad thing that could happen that involves the DNS is intractable. We need to do some high level systemic analysis as a baseline to start. So you probably would not want to get down into the gray area, in my personal opinion, very much.

Wendy: Thank you.

Greg Rattray: So I'm going to go there and then I'm going to go back this way.

Unknown male: I have a couple of comments and maybe one or two questions.

First of all, this from my experience previous, CERT is a trademark of CERT/CC, have you checked if you can call this project CERT, DNS-CERT?

Greg Rattray: I'm going to let Yurie answer that because she's on the Steering Committee for FIRST and well versed in these sorts of things.

Yurie Ito: We are communicating with them and I am aware of the trademarking. So we are talking to the CERT/CC, we have already notified that there's a potential we're using this, you know, CERT.

Unknown male: But it's international, a (inaudible 00:28:06) is CSIRT, Computer Security Incident Response Team, it's…

Yurie Ito: I'm aware of those…

Unknown male: So please check this.

Yurie Ito: Yes, we are checking, thank you.

Unknown male: And next is also, for me, it looks like DNS-CERT should not be operating CERT. Because there is not much work to operate incident on that. It should be like CERT/CC, coordinating CERT. Mostly producing documents advisory and this also clear that at least DNS-CERT specific organization will be to the level of regions. Like Europe, America, Southeast, South, North. So in this case, a major impact and work of DNS-CERT will be producing very consistent recommendations and advisory. Have to deal with this.

Also, at the next meeting, it was told that actually project of DNS-CERT will require only few full time personnel at ICANN or IANA, and all other will be located to the regional CERT that will be actually acting in coordination for handling incidents. At this presentation I haven't heard this. Because this is what would be logical. Three staff and all are sharing on duty-sharing cycle.

All over the world. In this way organize the most effective work and CERT in many countries. Actually this but if you want to comment but because I have one more.

Greg Rattray: I think I'll let Yurie, who I know has some thoughts, answer first and then based on that I may have a couple of additional thoughts. Yurie, you want to go?

Yurie Ito: So I think the business case has also described this as more coordination center coordinating, acts like an incident manager. When the incident or threat identified affecting to a large community as an incident manager quickly identified who's the expertise, where's the expertise, working with them, collaborating with them, coordinating with them, and facilitate the response. And bridging that resources and remediation when it's made, pushing to the operators where they need.

So that's, you know, coordination center role. Definitely that's, you know, going to be a very primary mission of the DNS-CERT. And your point about global operation of cloak-wide…

Unknown male: Sharing…

Yurie Ito: …sharing, that's also been a design of the full-time staff.

Unknown male: Okay.

Yurie Ito: That's a very good idea.

Unknown male: It keeps budget down and also more realistic structure.

Yurie Ito: Yes, yes.

Unknown male: And one more.

This may be simply comment. Actually, I understood that you made the consultation only with CERT/CC? CERT/CC, only made consulting this CERT/CC.

Greg Rattray: No. No, Yurie may be better equipped, but we are running an active dialog with FIRST, the global forum on incident response security team.

Unknown male: Yes, FIRST and ENISA, European…

Greg Rattray: Yes, we are in active, we've talked with them just as early as yesterday.

Unknown male: Yes we have CERT European?

Yurie Ito: Yes, we did.

Greg Rattray: ENISA.

Unknown male: Yeah, at least. ENISA is very important because I notice that in the comment area for this document, two documents that were produced, there is only one comment. So this means that nobody knows about this project, this initiative.

Yurie Ito: Comments coming in yet..

Greg Rattray: Right. We have talked with ENISA and we actually talked with them at length because one of the ENISA people was a trainer at the first ICANN-sponsored cyber security training for the standup of the East African CERT for the past four days. So we're pretty fully engaged with ENISA specifically and I think more broadly, the CERT community, we've briefed a number of times, most recently in Hamburg at the European Technical Meeting about the notion of a DNS-CERT and trying to establish, you know, how we can leverage the existing CERT capacities in order to scale this properly and not re-create things that CERTs are doing. And a strong notion that we will, national CERTs should be the first point of, you know, contact for a ccTLD operator and they just need to be equipped with the right skills to deal with DNS security issues.

I will say that the other, the next step, and again, in order to scale this thing to the value-added activities, is we plan to get all of the organizations, both CERTs and DNS-OARC and other security organizations, together to do a scenario-based analysis of what is actually required of this CERT in addition to the things that they already do so that we're not doing things that other people are already doing.

But you know, we're going to be challenged, it's good that we have a lot of participation, certainly those that want to let this session run a few minutes over, though Yurie will probably have to go. You know, I'm willing to keep going on the questions.

So coming back up the table this side, I see no more on this, the person in the light blue shirt? With the apple? So…

Unknown male: Thank you. My question is about the procedure and concerning the asking for commentary from the community. Someone asked me in Italy, "Why we didn't see so many answers?" And my answer was that in this meeting in here, certainly there would be an explanation by ICANN and then maybe you will get answers after the meeting, even numerous I think from Europe also.

But the point is, how do you see the process going on? The interrogation for comments is ending at 28th of March, if I remember.

Greg Rattray: Correct.

Unknown male: And then what do you expect from, let's say, that date and the next ICANN meeting in Brussels, because it is clear that the studies that we read are a draft, let's say, with some ideas that and the community would like to have a more specific plan and more specific goals and so on. So I suppose that you take some time in order to produce a further version of this and to understand how the community could compliment what you are proposing. And in the same time the answer to the question where the money is coming from is also another question that is asked by the commentaries. Thank you.

Greg Rattray: I see at this point, you know, to be reviewed and validated by, you know, the more senior leadership. We'd do three things. We'd do an analysis of the commentary we received, you know, after 29 March. Again, we plan to engage in a, you know, scenario-based requirements and operational, you know, procedures analysis with the key stakeholders and, you know, potentially get as far as to, you know, list specific initial operating requirements and a concept of operations, hopefully prior to the Brussels meeting. You know, posting it, a much greater level of granularity, you know, how this thing, how such a thing would functionally fit into the existing system as well as what would it do, you know, and what resources would be required. I believe, you know, although I don't have validation that this will occur, I also need to engage the Board on these issues of organization and resourcing and I'm hopeful that that will occur, but can't commit to it, you know, prior to the Brussels meeting. So, you know, I think that's my projected way forward.

Alan? And then you Steve.

Alan: Okay. My name is Alan; I am from African region, so. Just to say that in our community, I think our community is part of what we call a resource constrained. And I think it would be different, we don't have in our region, we don't have a cc coordination center in the countries so people may need to get information directly from this CERT if you're going to, so I think you need to think in how you can design this thing to meet the various needs of the region because we have different region and different needs. So as I said, we don't have cc's so many countries in our region, so don't target them who use the local cc to send information to the community. I think it will change but for now I think there is a need maybe for our, for some constituencies to directly get information from the DNS-CERT, central point. And we are working to share information in our community to ask our people to comment which we have a couple of weeks before the end of the comment times. And we appreciate the idea and thank you.

Greg Rattray: I think the only response, and I think Alan you know this, we just want to hear that voice as we start to define operational requirements and processes so that we can ensure that we meet the need that you identified there.

Steve, I think you had the next one? Oh, Lesley, okay.

Lesley Cowley: Hi, I'm not sure if that mike's working, yet it is. Okay, thanks Greg. Lesley Cowley from Nominet, the .UK registry.

It was interesting, as a manager coming to this discussion, because I'm not a security expert and I would never admit to being one. But Initiative One to me seems extremely sensible, looking at the gap analysis, looking at what's currently going on, particularly in terms of contingency planning. And, as others have already highlighted, there's a lot of that going on in some areas of the community already that we could more proactively share for example and learn from others without all reinventing the wheel.

And there is an opportunity there, I'm sure, for better coordination with some of the national agencies more globally too.

And I hear a lot of community support for that. But I hear quite a few rumbles within this community about the CERT proposal because it almost feels as though that is being pushed forward in advance of that analysis that might demonstrate the need and whilst there is support, both within the Affirmation of Commitments and the Strategic Plan for building on the security and stability role of ICANN, don't assume that that means widespread support for this initiative and that gives me concern. Particularly when you look at the proposed budget line, which of course will draw a lot of attention and comments.

So I kind of wonder the extent to which this is going to be actively supported within the community and whether strategically it might be better to build up that support more over time with the Number One Initiative actually feeding and informing that discussion that hopefully results in the outcome.

Greg Rattray: Thank you Lesley. And hopefully we'll see a lot of vigorous comment on these so that we can test the waters in the way you've described.

Steve?

Steve: Thank you very much Lesley. Two things, one is a question for clarification and the other is a specific comment.

With respect to the system-wide analysis of DNS, are we talking about just at the top level? Or are we talking top to bottom? Because I haven't yet understood, maybe I haven't been paying close enough attention. Are we talking about all of the DNS operations that are run by organizations and enterprises and independent operators or are we just talking about the DNS operations that are run by the top-level domain providers?

Greg Rattray: So, my sense is you will have to include a voice or an understanding of the, you know, the intersection between the top-level and enterprises and individual users, otherwise you know, you would artificially constrain what is systemic. You know, the challenge, and it gets to, you know, the bounding of this in a tractable is, you know, I don't think you can deal with individual risks, right? Or, you know, even enterprise level risk? You need to try to understand, you know, if there are systemic issues at the enterprise or individual user level. So I'm not sure that's a clear answer but I guess to the extent to which it is going to involve understanding risks that go throughout the system down to the user level, I think that should be part of how we approach the problem.

Steve: Thank you. Let me just leave that hanging there and then move to a different thing.

In the analysis of the Conficker and the subsequent kinds of activities, the technical issue was that DNS was being used as a communication mechanism for the control of these bots. And as you said, this morphed from an initial use of just a couple of top-level domains to 110 top-level domains and focused on top-level domains that were perhaps more permeable or more susceptible to exploitation than others. I remember from the discussions that we understood, at least in the abstract, that the use of DNS for that purpose was one of several possible similar mechanisms that almost any system that provided open registration. So we could be talking about Facebook or we could be talking about some other form of socially open system that allowed many, many people to join in and it would not have to be a domain name registration per se, it could be a comparable mechanism that is quite separate. So the question is, if we put all of this energy into trying to understand how to prevent Conficker and its successors, is that too narrow and is the problem sort of bigger than that? In which case, mounting this effort may be, however expensive it is, may be sort of not matched to the broader problem that's actually out there and that it's not just a DNS problem. So we might want to back up and take a much broader look at this and join forces across a much broader community than just ICANN or just the DNS community.

Greg Rattray: Steve, I understand that and that's been a constant portion of the dialogue that we've had. Clearly this is not a panacea for, you know, botnet propagation or any Internet threat, because there are many mechanisms. We've received pretty strong feedback from the incident response community that a hub around being able to coordinate the Domain Name System is part of the broader set of activities or challenges that are underway would be useful.

Taking a different slice through on it, certainly ICANN's remit only extends to the Domain Name System so within its responsibilities, you know, it's trying to pursue with its community, you know, what is its responsibilities in an effective, you know, approach to, you know, executing those responsibilities when it comes to response activities. So, my personal opinion is that there's enough within the DNS to focus some sort of collaborative response, the form of that to be determined by this dialogue.

I'm going to take one from chat room and then go down to the end of the table and then back to the one…Okay.

Rudolf Mayer: Thank you Steve. My name is Rudolf Mayer from SIDN, the registry for .NL.

I have a question about the CERT idea. One of your slides showed something like an inventory of existing organizations being active in some parts of the field. Before ICANN drew up this plan, did you actively go into a dialogue with these organizations and what they thought of this plan and if they would support it?

Greg Rattray: Yes we did and they've seen that matrix itself and the characterization of their efforts in that matrix.

Rudolf Mayer: I ask the question because I notice like Lesley in environments where I come that there's a growing, let me call it antagonism against this idea and very much that antagonism is being fed, I think, by the idea that this is an individually created idea of ICANN. Would it have been, I think it would have been much better if you had come up with a joint proposal supported, actively supported, by those organizations. Is there are particular reason why you didn't?

Greg Rattray: Again, we consulted with all of the organizations that are listed on that and none of those organizations thought we should not launch this initiative. Now, you know the notion that we should have co-branded in some sense, the notion of a DNS collaborative response or CERT capability, is I think probably a valid one. We're probably beyond the point that we can go back and do that. You know, I would hope that each of those organizations would weigh in positively or negatively on, you know, whether they think this is a good idea. I think that most, if not all of them plan to participate in this operational requirements and you know, operational processes workshop, so that how this organization would interface with those existing efforts will be discussed with them directly, you know, we hope in April. And the output of that will be, you know, will be available for the community as a whole to look at.

Rudolf Mayer: Okay. Well I agree you can't go back to that phase but it might really help you if in this present phase, if you could actively get those organizations to voice their support and to make clear that they are going to contribute to the idea. I think that would really help in getting the support for this plan.

Greg Rattray: Yeah, I think that's fair and I think we'll take it on board to say that as an output of this meeting, that has been requested of those organizations and we're going to actively seek their comment on that.

So I'm going to go down to the end of the table because I know there's someone who's been waiting patiently. And I know I also have comments in the chat room, so…

Mathieu Weill: Thank you very much for the interesting presentation and a very valuable discussion on this strategic, by definition, issues.

I'd like to really support Lesley's suggestion. Oh, I haven't introduced myself. I am Mathieu Weill, from AFNIC, the .FR registry.

And I share Lesley's suggestion that maybe the current situation, it's strengths and weaknesses should be further investigated before launching a $4 million dollar project on the table.

I am also echoing Rudolf's comment because AFNIC happens to have a member who is in the OARC Board. You've mentioned OARC. And my understanding of the reactions from the OARC community to this proposal was that – antagonism could be a word – at least, support would not probably be the word I would use. And so I urge you to get the actual written comments, I'm sure it will come, before the end of March. But I think it's important that you take these into account in the course of the project.

My question then to you would be that my feeling from the gap analysis that you've been doing is that you have identified holes where you would like to fit in. And one of these seems to be the ability to coordinate all DNS operators. That relies on the ability to get in touch efficiently and reliability with these operators. And my feeling is that a number of people have already tried to do that. And they failed. What makes you think that you would have the ability to succeed where others have failed in this field?

Greg Rattray: I will give a pretty direct answer to that. In the Conficker worm situation and when the Conficker B morphed to Conficker C and 110 instead of 9 registries were implicated, we were asked and managed to, reach all 110 successfully of those registries and implement blocking against the domain names that were going to be utilized in Conficker C. Basically I think due to the fact that the IANA database and its upkeep requires ICANN to be in contact with every ccTLD operator. So we had one, admittedly it's one and it's anecdotal, one very practical, you know, success story in that regard, in terms of, which again, this is, the CERT is not conceived as an ICANN function. You know, and I agree with you that the success of such a CERT would be based on the buy-in from people so that they would be contacted and the information would be shared. But I do think we have a practical example of success on the challenge that, you know, you highlight there. Again, it's one, it's not necessarily repeatable, but I think we have one there.

I would like, again, in the notion of utilizing remote participation, Liz, if we could grab those questions from the room?

Liz: Yeah. The first is for either Greg or Yurie from Rick Wilhelm.

"Can you comment on any feedback from the various existing organizations that currently support security efforts from the list into 2.8.3 and the paper?" He is particularly interested in the response of the DNS/OARC members.

Greg Rattray: So let me go to that because that comment was also made at the DNS Security Symposium we held in Kiyoto in February. There was at least Board member and I think more, of DNS/OARC as well as Paul Vixie who is not currently on the Board, but was the, you know, basically generating force behind DNS/OARC out of ISC.

I would hesitate to want to, you know, given that their feedback to us was in private, and this is a public consultation, I'm really very hesitant to, you know, try to specifically characterize what they said. I will say that all of them thought it was a legitimate exercise to explore certainly the relationship between a DNS-CERT and DNS/OARC, and again, where a DNS-CERT fits in an ecosystem of existing security organizations and, you know, what value-added it could have, and again, we plan an early April meeting with all of these organizations to define, based on scenario analysis, you know, where a CERT would add to the existing sets of activities and try to be very explicit about that.

I think, in light of this discussion, I may ask the participants in that workshop to make the deliberations there publicly, you know, to be able to publicize in some fashion the nature of those deliberations as well as you know, what we find as the output of that. I can't predetermine that that's going to be acceptable to the people that we have at that session.

I'm going to go down the table and then back to remote participations.

Oscar Robles: Okay. This is Oscar Robles from NIC Mexico, the ccTLD for Mexico, .MX.

My initial reaction to this idea was that it seems to be a good idea because there is this gap of DNS coordination requirements globally. But when I see the budget, something starts to change in my mind. Even if you give me $100 million budget, I could come up with a better idea than this one, maybe because that's a lot of money. So rather than going through details of how is this $4.2 million is going to be spent, I think that what I would ask you is to come up with a detailed set of goals and measurable objectives and concrete and clear, that could give us an idea of what is what this group is proposed to actually comply. Because at this moment, it seems to be too wide and I don't know, maybe in three years it won't be $4.2 million, so it would be $20 millions, and it's a never ending story of organizations with huge budgets and missions with no clear and concrete objectives.

Greg Rattray: So I think that's, you know, in congruence with other comments, I think, you know, adding the weight to the detailed, you know, mission requirements and then therefore initial operating capabilities linked to the necessary resources for those capabilities. We are committed to do that in the April timeframe and try to publish prior to the Brussels meeting a more detailed list of requirements, objectives and then, you know, how a resource build fits to achieving those objectives.

And we have one more in the chat room?

Liz: This is just a quick comment. I think someone notes that regarding the contacts with regional CCERTs, that there's an upcoming meeting the 30th – TF-CSIRT meeting 20 and 21 May, 2010 in Heraklion, Greece and there's a link provided in the Adobe Connect.

Greg Rattray: Thank you.

Unknown male: This is a comment from me.

Greg Rattray: Yeah, we have one more comment at least.

Unknown male: I sent this information.

Greg Rattray: Oh, OK.

Unknown male: It's quite useful that Yurie will present this idea at the European TF-CSIRT meeting and also it is at the same island in Greece that ENISA located, situated. So end of May – and to this people, people in this community – make a very strong scrutiny against this proposal. It looks like very, very, like draft, especially in the budget part.

Greg Rattray: And I will say on that last comment, I had the inclination, we could have engineered this to a greater level of granularity, but when you do that, you start to have gone down one road and not another, so this proposal was shaped at a fairly conceptual level to allow a phase of feedback which we're obviously receiving at this point. Again, we plan to do a multi-stakeholder mission analysis.

In terms of engaging both ENISA, that's certainly on our near term roadmap. We plan to meet with the new Director General, I believe, of ENISA and we again, his CERT person was at, or yeah, CERT person was actually in our training the last four days here in Nairobi. Again, Yurie is an active, or she's on the Steering Committee of FIRST, including the regional and attends the regional forums as well. We're certainly willing to give a briefing at the Greece TF, it may have to be remotely. I have planned to engage, you know, there as well.

With that, we've run long probably. I'm going to have to cut this off. This has been great in terms of the amount of participation and feedback we've received but seeing no more.

Oh, we do have one more.

Unknown male: Just a short commentary about the expectations concerning the funding model because I think that this is an important aspect and from the document that was produced by ICANN, apparently the $4.2 million, ICANN says that it will provide the funds to start up the DNS-CERT and then hopefully this should become a self-organizing and self-funding body. But of course, the community is starting to understand or is interrogating about how to reach an independence and how the funding model will function. Because for what regards to the ccTLDs, of course the security is one aspect that is part of the service that they offer. But then if we invent this supra-national coordination body, this will have to find ways to sustain and to find a sustainable model and one option is solidarity by all the agencies that need some overall coordination but such kind of funding models rarely function in a satisfactory way. So an elaboration about that is quite important. Thank you.

Unknown male: Yes, I had a question about the, what I call the security audits portion, the stuff for the AoC, $2.1 million. I didn't get from the paper whether ICANN conceptually is planning on doing that work themselves or whether they're considering hiring that work out. But in most cases organizations hire that work out in order to maintain independence and it wasn't covered in your conceptual paper.

Greg Rattray: I think we may be mixing two things. Under the Affirmation of Commitments, ICANN will receive a review that initiates in October of this year. That was not at all part of the Strategic Initiatives except for the fact that, you know, the Initiatives are the types of things we think might be, you know, in-scope for such a review, is ICANN doing these sorts of things, contingency planning in particular being explicitly identified. The Board is considering approaches, you know, and it's going to have to do that in conjunction with other parties that have a role in these reviews, about how those Affirmation of Commitments reviews will be conducted. And, you know, again, that's not part of the Strategic Initiatives. So I think that's where your question was driving and I think how we conduct the Affirmation of Commitments reviews is under development. It's actually the subject of a separate session here at the meeting.

And I think with that, barring anything in the room, Liz? We have concluded.

I will say I appreciate everybody's attendance here at this session and the robust dialogue. I will say that my personal expectation was that, you know, we would get a lot of feedback and that we are, you know, required to define both in more detail and analyze the value-added of these initiatives in conjunction with the community. And the extent to which we can get those written sorts of comments in, that's a very useful thing.

So I thank everybody and I look forward to working with you further on this, to the extent to which it goes forward.

Take care.

(Applause)