RECORDED VOICE:	This meeting is now being recorded. [AUDIO BREAK]
JENNIFER BRYCE:	Hi everyone. Welcome to the room. We're a couple minutes early, so I'm just making some noise just because I noted Kerry-Ann's comment that she couldn't hear anything. So it was actually no talking so I don't know if you can hear me now, but anyway, feel free to dial in. [AUDIO BREAK]
UNKNOWN SPEAKER:	Hello.
JENNIFER BRYCE:	Hello.
KERRY-ANN BARRETT:	Hello.
KERRY-ANN BARRETT:	Hi. Can you hear me now?
JENNIFER BRYCE:	Hi, yes. We can hear you. Welcome.

Note: The following is the output resulting from transcribing an audio file into a word/text document. Although the transcription is largely accurate, in some cases may be incomplete or inaccurate due to inaudible passages and grammatical corrections. It is posted as an aid to the original audio file, but should not be treated as an authoritative record.

KERRY-ANN BARRETT: Okay. It's now working on my phone.

JENNIFER BRYCE: Okay, everyone. So we're at one minute pass the hour. I think the other two members of the sub-group we're possibly waiting on, are Matthew Goro and Denise. So we can give her a couple more minutes and then the way that the sub-topic groups calls run is, I guess Kerry-Ann, you're rapporteur so you can either lead the call or make a decision amongst yourselves how you want to do the call. We haven't got an agenda. We just put the document on screen for the topics that were initially discussed in Madrid and I know there was some more discussion in Johannesburg. But from this point on I'll just leave it up to you all to have your call. [AUDIO BREAK}

ERIC OSTERWEIL: Hey Jennifer, this is Eric. Do you know from -- Denise was planning during today, did she send any regrets or anything?

JENNIFER BRYCE: Yvette, do you know if Denise sent any regrets?

YVETTE GUIGNEAUX: Hi Eric. This is Yvette. I don't have any as of on him. I think she was planning to join. But I know she had some Adobe run issues of trying to get in here. So she may be trying to connect but I don't have any regrets as of yet from her.

ERIC OSTERWEIL: Okay. So I’m not sure exactly whether -- have people had a chance to look at the document that's being displayed now in advance of today? I can't remember if it got sent around but I think it's the work product from our last face-to-face.

KERRY-ANN BARRETT: Hi Eric. Can you hear me?

ERIC OSTERWEIL: Yes.

KERRY-ANN BARRETT: Eric, I looked at it but I think because I wasn't able to join in to the meetings during Johannesburg I don't know if you mind leading today and then I'll take the notes and then circulate it by e-mail to the ICANN staff so they can at least upload the notes from this call, cause I think it's more assimilating ourselves as to how we plan to proceed with the work in terms of summarizing our discussion, dividing any other research or review of the material that we need to answer the questions.

` I'm always okay generally with the questions that were posed because it was similar to what we discussed when we were in I think Madrid and when we started to think about this topic in Copenhagen.

ERIC OSTERWEIL: Right. Okay. Yes okay, that's fine, I can do the leading. So can someone unlock the presentation for me so I can make a mess of things? Thank you very much. So let's see. Yup. Okay. Just trying to get the hang of this. Hold on a second. Okay, I think my computer is having an issue. Let me just -- I'm great. Now I'm totally lost where you all --- there we go. Cool. All right, problem's fixed. Okay, cool. Yeah, so let's see.

My recollection, and I believe this will be borne out by the document here, was that we broke things into sort of high level categories and then we broke things down into things like Attacks and whatnot. So I mean this was really kind of a straw man. You know, definitely could use any input that other people have, so let me try and find the part that I was actually thinking about. Like for example there's a section in here somewhere where we talk about like DDoS and stuff like that. Right here [inaudible] of registry back in operational [inaudible], multitudes of victims, DNS, DDoS.

So I guess one of the questions I have for the group now that there's sort of more of us sort of plugged in, is you know, despite having already asked but I'll sort of ask again, do we think that this is at the right level and the right sort of scope for the sub-team that sort of -- the Future Challenges sub-team? Or do we think some of this is too far over the horizon or some of it's too near term or do people wanna go over it; like if not everyone's had a chance to look at it, one of the things that we could do is we could sort of go through it.

Sorry, I was just reading comments in the chat room. Okay, so it sounds good. So you know, if you all want, one of the things we can do to spend our time, is we can start off by reviewing what's here and I think that'd be advisable if people haven't had a chance to look at this yet and if people feel pretty secure that they've got a sense of it then we can jump right into sort of, you know, discussing it. So I'll ask for a poll of who thinks that we should start off by reviewing what is currently listed in the product?

DENISE MICHEL: Hey Eric, this is Denise. Apologies, I'm not able to get into Adobe Connect yet. So let me share that I think a quick review of what we have in the list so far would be a useful thing, and I guess I'm not as concerned about whether it's too far in the future or not. I think more concerned about I guess working towards consensus on that we have reflected what collectively we're trying to be the most important and impactful future challenges for ICANN.

ERIC OSTERWEIL: Certainly, that makes sense. How's everyone feel about that?

KERRY-ANN BARRETT: Eric, this is Kerry. I agree with Denise. I think what would be really useful as well is not to necessarily remove everything from the list you have as we go along in the review, but we should actually raise it as these are the things that we think are concerns that ICANN should think about in the future.

These are the things that the sub-group focused on in terms of more details but they should keep it on the radar as they go forward and probably have it subsumed into other reviews if not under ours. Some of the other review teams that they may have at least the work will continue cause I think the list is a pretty good list especially on the technical level.

ERIC OSTERWEIL: Okay. Does anybody substantively have comments that would suggest we should go back over this list? Or does everyone pretty much agree with Kerry-Ann? Anybody who thinks that we should -- okay, so I see a request for a review. Okay. Well so, we can sort of maybe spend just a few minutes going through it so it doesn't become kind of like a re-insession.

But yeah, I realize not everybody was able to attend the face-to-face and so that was why I was asking if people had any chance to look at the document. Okay, so -- no, no, not at all, not at all. So if you sort of look at what's currently being displayed -- so Denise, I think Denise is the only person who's unfortunately not able to get into the Adobe Connect, so's everybody else seeing -- oh Steve, I see your hand's up, go ahead, please.

STEVE CONTE: Hi Eric, morning. Thanks. Just to ask a question of clarity -- is this list comprehensive of what was discussed, I think it was you and Denise, in Johannesburg? Does this cover what you guys worked on in Jo'burg?

ERIC OSTERWEIL: I believe so. I think Denise is probably going to have trouble verifying that herself until she's able to get into the Connect room, but you know, in sort of scanning it, it looks like a good sort of digest of -- I think we initially did a couple passes of scratching down our thoughts and so I think this looks a little more [inaudible] some. Maybe as we go through it real quickly now, if anything jumps out, then we'll just sort of make a note of it and circle back. Does that make sense?

STEVE CONTE: Yup. Thank you.

ERIC OSTERWEIL: Okay. So, as the sort of description activity sort of starts off you know our goal is to sort of get a longer view of what's going to be important so that's why we don't wind up for example through our sub-teams being focused on things that are here today at the expense of the report having utility down the road which I think is also kind of in concert with what Kerry-Ann just said.

So there's a sort of a five bullet list at the top that talks about just kind of a brief methodology how we might approach this so how do we set speech challenges, how to you know, we'll need to explore you know forecasting research and I think in the space of our internet unique identifiers that ones that fall within our purview. What have been or could be impact of the evolution of numbers and types and [inaudible] in the DNS, so you know, this would sort of I believe -- so you know, Denise [inaudible] keep me honest on that all the stuff but you know, this will sort of be one of the places where we'll understand the way things we use now will pay attention to things that are coming both through briefings and our own expertise to know how this will be important. How we suspect this might be important future, whatever it is we're looking at.

And then, you know, in reviewing the ICANN security efforts I think we'll just want to be able to be cognizant of what the other sub-groups are doing so we don't replicate work but you know certainly I suspect there'll be some dysfunction between the security threats that the -- another couple sub-teams look at them, what this group will look at.

So again we'll just sort of try and stay on the same page with everyone else, and then you know as new technologies emerge, there's increased chance for the identifier systems that are in existence today to be used in ways that they haven't been foreseen in the future. And so we'll just have to be careful with slippery slope not to sort of wax poetic about things that take us off into the bushes. So those are the sort of high level framing objectives from the group. Does anybody have any comments or questions? Okay, Kerry-Ann, go ahead.

KERRY-ANN BARRETT: Eric, just to add to the final sentence of what you said, I think it's important to note that because the technologies are moving so fast, I think like a sub-group we need to put that as a, not a disclaimer, but a caution recognizing that while we may know that these are the proposed [inaudible] for the future for the DNS, we recognize that things may evolve and change. So I think if we find a way how we could have generic security recommendations that would apply to any form of technology going forward.

I think while we look at this as well, looking at emerging technologies and certain threats that will be evasive no matter what the technology that is there, and I think we need to look at those kind of future [inaudible] challenges as well. So for example, if it is that there is certain platforms that are being used and there is no regulations in place that there is no basic security testing as the technology is being applied, those kind of generic best practices so to speak, we could probably highlight those as well.

ERIC OSTERWEIL: Yeah, that makes sense. Yeah, I think that makes sense. I think it goes without saying that you know, we'll understand that you know, in looking sort of like in our scope and terms of references looking broadly we understand that recommendations we come back with will have to be made so that they follow the purview of ICANN. Nevertheless, I think your point is well made that we will necessarily need to look a little broadly especially when it comes to future challenges.

Does anybody have any other thoughts on that? Okay, cool. So let's see. So the new items to discuss they just kind of serve, you know, kind of [inaudible] that a little bit, so a middle where research emerging technologies, internet governance, and privacy regulation like GDPR maybe becoming present. But nevertheless, as far as new items to discuss, does anybody want to add to that because we may be able to sort of really focus up on those and four of them I suspect could easily draw the rest of our time or maybe not, but potentially. Certainly I don't want that list to be considered comprehensive as other people other thoughts.

So if we were to for example try and close those off in the call today, does anybody feel like we should be adding anything to that or taking anything away potentially? So Kerry-Ann your hand is up but was it up from before, is it up again? And then I have -- okay, cool. Then Ameen, yes go ahead.

NOORUL AMEEN: Can you hear me? Hi.

ERIC OSTERWEIL: Yes, hey.

NOORUL AMEEN: All right. So, a quick comment on the list that is mentioned of the attacks. I can see clearly that these are current things. So current situations, current types of attacks and dealing with these attacks is the responsibility of IT security which probably fits under group number one. Like maybe DDoS, router injection, like BGB stuff. It's all part of IT security operations at ICANN and there is a high probability that measures are already implemented towards dealing with such types of attacks.

Same for social engineering or DMS zone file attacks, I can see the list. So how are we going to focus on future challenges if we are trying to deal with current attacks? Should we have descriptions that go more towards projecting what these types of attacks could look in the future? Is this what we're trying to reach?

UNKNOWN SPEAKER: So I'm unhappy that I've to respond to that unless somebody prefers to go first. I don't want to monopolize the mic.

ERIC OSTERWEIL: Okay. I'll go first and then I'll watch for hands. So I think that this is a sort of a very good point that I think there -- one of the other sub-teams is ICANN SSR. Another sub-team is DNS SSR and it's reasonable to assume that those teams they'll be completely read out to the other groups. So it shouldn't be a mystery. It's just you know they'll be moving in parallel. We'll address issues and perhaps that are existent today.

So like a social engineering attack, to compromise like for example the algorithm deployment, that might have less to do with global DNS security just because it would be sort of a focused attack on like, you know, INFOSEC. It might have more to do with ICANN SSR's remit which is the sort of you know, check the plants to make sure they got proper controls in place, to remediate blah, blah, blah; have an IR team, have [inaudible] whatever else.

So my guess is that those very specific attacks might be addressed by another team. The very broad attacks that we see today, might be addressed by the DNS SSR team. I think one of the sort of the nuances we might be trying to do is whether DNS gets used in a new way in the future, or a new protocol system behavior or something shows up to use DNS that exists, a facility DNS today in a different way tomorrow. Do those expose new attack surfaces and I think that [inaudible] is sort of one of my canonical references. But I see Denise's hand's up. So I mean, before that --- Mohamad, does that sort of answer your question at all? Or does it still leave it kind of open?

MOHAMAD AMIN HASBINI: We'll just discuss further as we go on. Thank you.

ERIC OSTERWEIL: Okay. Yeah, Denise, go ahead.

DENISE MICHEL: Yeah, so on the last topic. I think it's a really useful one for this group to get it hands around. I guess in my mind I see the division as the other sub-topic group assessing the current effectiveness of, you know, OCTO Middleware research and current challenges in current activities that are occurring right now whereas we're looking, we're trying to project five, ten years down the road and look at whether, is ICANN aware of the future challenges. You know, do they have planning and other resources in place to address it and does the team have recommendations that we think would be useful to ensure that ICANN is looking down the road at what we feel are some of the biggest challenges that we expect it to face.

And then jumping back to Eric's question on the four items, I think internet governance issues is quite broad. It's a very large umbrella. So I think it would be useful for this group to be more specific about what we're going to look at within internet governance issues. Similarly I think perhaps new regulations in GDPR I think it would be useful to flesh that out a bit more and be more clear about intersection with SSR and also of course ICANN's objective. I think the latter two I think in particular, would be useful to be more specific because that could be quite broad. And then on the emerging technologies, I think the paper that we reviewed in Madrid by Dave Piscitello and Lisa Piper, strikes me as a really useful stepping off point. I'll stop there.

ERIC OSTERWEIL: Okay. Yeah then, I think that makes sense, Denise. Mohamad, go ahead.

MOHAMAD AMIN HASBINI: Thanks, Eric. One thing I'd like to suggest too is that we look at performance security future issues like especially when we talk about IoT devices and the increasing number of systems. We talk about limitations on some hardware on the providers' side. And that could also be one interesting topic to be actually researched and it could be a bit different than the attacks but it's also for securing availability of services. Thanks.

ERIC OSTERWEIL: Okay, that makes sense. Denise, is your hand up from before or is it up again?

DENISE MICHEL: Sorry, it's old.

ERIC OSTERWEIL: Okay, all right. Okay so maybe we just -- Steve, hopefully you grabbed some of that stuff for the notes, some of the sort of suggestions. So unless there are other suggestions -- Kerry-Ann, I see your hand is up.

KERRY-ANN BARRETT: Thanks, Eric. Just one thing that I just remembered. When we went to the DNS symposium, there was one question that they weren't able to answer really clearly cause when Mohamad spoke awhile ago, it reminded me. I'm not seeing where we're looking at the management of [inaudible] provided contracts in terms of how the legal unit actually reviews this contract and how they build in, not even that, how they build in the monitoring aspect of it in terms of the security provision by subcontractors.

So I don't know if probably where we have how effective are ICANN security efforts [inaudible] preparation for future threats, maybe we can also examine the contract management process and how they actually keep their contractors and sub-contractors of contractors accountable.

DENISE MICHEL: Kerry-Ann, this is Denise. I'm sorry, I'm away from my laptop to raise my hand, Eric. Just a clarifying question if I may. Were you referring to some like the contractors and sub-contractors in particular areas or just a broad you know, process relating to any contractor or sub-contractor?

KERRY-ANN BARRETT: I think it was more specific to what Mohamad spoke about in terms of the provision of hardware and software. The contractors that actually provide the base operational instruments or the framework or the infrastructure for the DNS, to see how they manage those contractors. It's more to look to make sure that they have at least clauses that speak to the requirements for them to have certain security inbuilt in the provision of the services they have. And that the stage of the cost of proposals or at the stage of the actual contractor that [inaudible] to the selected contractor.

DENISE MICHEL: Okay. And of course some elements of the DNS there are no contract. Did you also want to look at that?

KERRY-ANN BARRETT: No, I think it's [inaudible] you what is [inaudible]. It's outsourcing. I can probably frame it possibly more specifically that it's outsourcing.

DENISE MICHEL: Okay, I see. Yeah.

MOHAMAD AMIN HASBINI: Guys, one last comment, please. For part of my work on smart [inaudible] security, there is a lot of research around the vendors selection and this could also be an extension from the idea of assessing hardware and software to assessing certain --there is a lot of emphasis in the future environment or organizations around, but the process of selecting vendors or selecting solutions. So maybe we can highlight that as a way of securing ICANN because securing, it's also about evaluating the selection of these vendors, evaluating technologies that are going to be used and we can even go towards talking about techniques to avoid vendor monopolies or vendor influence towards the selection process in these type of solutions, future solutions, future technological solutions.

Another thing that we can also talk about is how SLAs are going to be implemented and how SLAs are increasingly being required from the vendors or from the solution providers. Or you can also call them contractors or subcontractors in this case. So we're talking about subcontractors but also outsourcing providers, but also solution vendors. Thanks.

ERIC OSTERWEIL: Thanks, Mohamad. I'm going to go ahead and jump in. I think it'd be useful for us, and I'll play the role of fun police or culture cop here. So let's be sure that we consider things broadly but always remember in our analyses that at the end of the day, if we're to come back with recommendations, they need to be recommendations that ICANN can actually ingest, that fall in its purview. And so we have to be aware that if we're going to look at things like vendors or SLAs with vendors, depending what you mean you might very well be talking about service providers that are far outside the purview of ICANN.

And so we wouldn't really be able to construct a recommendation for ICANN based on the open economy or the marketplace. That said, certainly it bears looking into and our job for ourselves is to, when we find an issue, basically figure out if there's a projection of issues that map out onto what ICANN has control over. So for example, if there is a vendor who runs a sub-train of the DNS as a result of a contract and that has nothing to do with ICANN's TLDS, it may be difficult for us to actually say there is a SSR challenge issue for ICANN unless we can say this is how it relates to the management, delegation, choice of, protection of whatever.

But I just want to throw that out there to bear in mind and I think it certainly does not limit us from looking at the things that you all are talking about but it puts the onus on us to be sure that at the end of the mapping, if we do think we found a future challenge, we have to illustrate how it relates in a meaningful way to ICANN. So I see Kerry-Ann and then Mohamad.

MOHAMAD AMIN HASBINI: Thanks Eric, let me quickly reply to your comment. I do agree we should avoid any type of evaluation of current SLAs or go into the discussions of SLAs with ICANN-related subcontractors or vendors. Though I do believe this is something that we can justify through relevant research and future challenges towards smart city or future organizations. What I'm actually thinking about is more related to developing a road map towards increasing ICANN consideration of pushing SLAs on vendors and providers.

So we can highlight this as a challenge, justify this as a challenge with relevant papers or relevant sources and then create some small roadmap which can empower ICANN towards better dealing, gradually increasing SLAs on vendors, etc.

ERIC OSTERWEIL: Okay, Kerry-Ann?

KERRY-ANN BARRETT: I totally agree. I think the idea Eric is not to go into probably vendor-specific contracts and look at the existing contracts they have to scrutinize, but ICANN should have certain template contracts that once they go into any of these arrangements, they're going to bring something that will actually cover the concerns we have.

One thing that I used to do is that I used to develop one of these clauses that could actually be used in any contract in this type of service. We can get specific recommendations, it may not be a specific language, but at least indicate to them that as a standard process, as Mohamad said, we don't think that you should consider especially as a future challenge because if you don't manage the contractual arrangements now, whether or not it's specific I can give recommendations to other persons to actually manage the DNS. I think somebody said earlier, how can we build it in to actually be able to manage what we anticipate in the future it's going to look like?

ERIC OSTERWEIL: Okay, great. I think as the sub-team was the title feature in it, we will have the highest level of scrutiny. So bear that in mind as we go forward. Okay, so I'm going to go ahead and just follow us through a little more on the plan unless people jump on me to sort of change things up. The next section in the document talks about the assets that are relevant to this sub-team. And so even just based on what we were saying just a moment ago, my suspicion is that this may grow. But principally, the statement of assets includes identifier systems that are implemented by, for example, the DNS. And that would include issues that result in, for example, hijacking, etc., and so forth.

There's a sub-bullet list in there that breaks up the specific items that are included. Authoritative domain name servers, recursive and stump resolvers certainly play a role, they may not be under ICANN's purview to manage but they're certainly a part of that. Time check, we're 25 minutes out. Thank you, Kerry-Ann. IP addresses and autonomous system numbers, this one is very complicated.

For example, ICANN doesn't manage any IPv4 but they manage almost all the IPv6 depending on how you actually describe manage. So that's probably a hour and a half discussion that I won't get into unless people really want to. But nevertheless, part of the identifier system that relates to ICANN -- protocol parameters.

So there's a number of examples of these but, for example, I entered registries for port identifiers like DNS Port 53 that's managed by an IANA registry which is manages as part of PTI. So that's all we have now but I'm guessing from what we were just saying, and maybe I can get an agree/disagree, that some people feel like that list may need to grow based on what we were just talking about -- contracts, SLAs, vendors, etc. So do we feel like that text needs to be augmented? Kerry-Ann, go ahead.

KERRY-ANN BARRETT: I think along with what Mohamad did, we can just give a general of one bullet point that would just cover -- I think Mohamad you called it a vendor management system because that would cover the SLA. That would cover all the contractor stuff [inaudible] understand. And then as a sub-team we can work through the specifics and kind of bullet out the other subareas because we can't go too wide, as you said, Eric.

ERIC OSTERWEIL: True. I think that sounds fine. My concern is just vendor management, it can mean a lot of different things. Actually, I wonder a little bit if we maybe aren't talking about the exact same thing. So it might be worth putting some text down so we can see clearly because the vendors that ICANN contracts with for various ICANN duties are different than, for example, vendors that help facilitate subtrees in the DNS.

Like chiba.jp has a whole host of domain names underneath it. It's a prefecture and it's managed locally inside Chiba, Japan and it has nothing to do with ICANN. So it's possible that what we're talking about with vendors might just need a little more discussion or at least If there is some text that gets put together it'll be clear whether we're on the same page or not because managing contracts that relate to the -- can you guys hear me?

DENISE MICHEL: Yeah, I can hear you.

ERIC OSTERWEIL: Okay, there was a comment in the chat room that wasn't being heard. So I think it would be worth putting some text out because vendor management could mean like quite a few different things and so I think it would be a good idea. Can I get someone to volunteer to draft that sort of bullet text in the spirit of -- take a look at the bullets that are there so we can have a sense of how much writing? Then maybe someone will go ahead. I'm watching the chat room and looking for hands. I'm not the rapporteur but I reserve the right to volunteer people.

MOHAMAD AMIN HASBINI: Hey Eric, quick comment here. I definitely do not think we should expand this to vendor management because vendor management would include also other measures. I think we could clarify certain things or point out certain things that we believe to be valid to be researched especially, for example, performance security and vendor security. And we can limit our work to that. We don't need to expand it more. Vendor management could include financial stuff or it could include maybe sales related information. That's not things we need to focus on. We need to focus on security-related issues.

ERIC OSTERWEIL: Okay, Mohamad. I took that as a volunteer operation by you to draft the text so I appreciate that. So that sounds fine. Just bear in mind that there will potentially be some scrutiny about how this relates to ICANN so just keep that in mind as you're going through and I think we'll look forward to seeing that. I'll try to move a little more expeditiously through the sub-bullets because the extent to which we like the outlined structure that's there, you may just want to add various pieces of what you were talking about to the various areas.

Like there's assets and then down below there's vulnerabilities and below that there's threats and then there's risks. I don't think any of this is capped in stone but it's possible that it'll be easier to structure what you're talking about by breaking out into subsections or not, I'm just throwing it out there. But regardless, thank you very much for volunteering, I totally appreciate it. No hands are up. So vulnerabilities, this is a section where I think we were sort of going to be talking about of the areas above, where are there problems?

So I saw a comment scroll by that I can't see now in the chatroom about prefix hijacks or something like that. But regardless, the vulnerability section would probably be where we would discuss if we thought that there was something that we wanted to dig into, it would go there. I would propose that treats are different than the vulnerabilities in the sense that vulnerability is for example an attack vector and a threat is actually an effectuated attack. And then risks, I think that's the sort of nice area where we could discuss what would happen if? So I like this structure, maybe other people see it slightly differently which is totally fine.

But I think it breaks up the components so that we can start analyzing them more clearly. So before we get into the actual attacks, does anyone have any comments or questions about that structure? And I see that there is a conversation in the chatroom for those that are on audio. Muhamad said that he's going to go ahead and provide some small vendor security text and performance security subsection. And then Amin said he's happy to give clarifications and Kerry-Ann said that she'll add in when he circulated the first draft. Okay, Steve go ahead.

STEVE CONTE: Thanks, Eric. Just to clarify because I think I have a misunderstanding of the sub-teams. I'd like to hear the sub-teams opinion on this. My understanding of the future challenges group was to look at future challenges, future threats that might affect the DNS and the unique identifier systems that ICANN manages. And not necessarily looking at ICANN as an organization. And during today's organization, it sounds like this section really wants to focus in on ICANN as an organization with contract SLAs, and that's fine.

I just want to understand that better. Where is the sub-team supposed to be looking at things such as things that could threaten the security, stability and resiliency of the DNS and unique identifiers in the future such as DOA or block change or other things? Or is it going to be a combination of both? I just want clarity for my own edification on that. Thank you.

ERIC OSTERWEIL: I'm going to throw myself in the queue but I see that Kerry-Ann has got her hand up first.

KERRY-ANN BARRETT: Hi, Steve. I think it's a combination of both. How, and I can be corrected; how I see future threats is actually looking at not just the technology and what technology can do and where the technology is going and what the direction of the technology, but it's to actually balance it with the management of that technology because we're moving so fast with the technology, advancing and improving the DNS and how it's actually managing the services that we can provide on the internet. But if it is that it's not managed properly, the [inaudible] technology and the management process is not complementing it, we end up in more disarray in the future.

So it's to actually predict how do we learn from this at the beginning as the technology is advancing to ensure that the structure that we've put in is not slowing it down or preventing it from performing the way it should be, but we actually have remedial measures in the future based on putting them in at the beginning. So it's just to ensure that we can mitigate. It's more as a future threat if we don't put the mitigation [inaudible] at the beginning. That's what I'm thinking, and I could be corrected, would be what we're highlighting. Other than that [inaudible] will cost us more.

ERIC OSTERWEIL: Okay, good. I see Steve acknowledged that that made sense to him and that sounds like pretty much what I was going to say as well so you said it probably better than me. Mohamad made comments and it's starting to sound like we're all becoming violently in agreement. So I'm going to sort of say that the proof will be in the pudding. When we start to see the text, it should start to allay people's concerns. But Steve, I think keeping us honest with questions and observations like that is very helpful so I hope you will continue.

So top identifiers system attacks. So this was something that when we were face-to-face, we were just sort of starting to put together. And I know we didn't consider it to be completely comprehensive, it's just sort of a starting point. And in fact, not necessarily everything here will actually be something that we will take to fruition. So this is just to sort of get our pumps pumped. And yes, 15-minute check. We're three quarters of the way there.

So round insertion attacks. So what could happen if [inaudible] were subverted in regards to the identifier system that people rely on from ICANN.

Coalescence of registry backup operators for multiple TLDs. So what happens when you put all your eggs in relatively few baskets? It makes for a high-value target, it makes for critical points of failure, maybe not singe but certainly fewer. It means that your software diversity potentially is reduced. So that means that a critical failure, a critical bug, vulnerability, etc., in one particular popular variety of software may affect numerous branches of the DNS if they're all run off the same source. It could mean that account compromises like Cloud Hopper kind of situations become more relevant, things like that.

So coalescence of registry backend, does that make sense? I'm going to just start to poll you guys as I go through it so I don't buffalo everyone. Did that sort of make sense or did that not make sense to anybody? Comments or concerns?

So the next one was identify hijacking via social engineering. This one we did wind up breaking up a lot of examples specifically of that. But

Mohamad, I think you mentioned something kind of like a survey adjacent to this as well. So I think these are actually opportunities also for people who have thoughts or questions to jump in and help annotate the documents. So if you see a section like identify the hijacking via social engineering and you can sort of illustrate how that has some kind of relevance to what we're talking about, maybe filling in or adding would be useful. DNS zone file attacks, what can be done by manipulating a zone.

And I think this could include potentially TLDs that are not signed by DNSSEC as secondary's. I think there's been a couple recent claims of concern about ccTLDs in that regard that I think may not have stood up to scrutiny but nonetheless might have illustrated a point. Mohamad, I see your hand up.

MOHAMAD AMIN HASBINI: Thank you, Eric. I'm a bit worried. I'll just mention my concerns and then we can take it from there. Identifying hijacking via social engineering -- these are things that we currently see and organizations are already trying it. So there could be new technologies that could be used in the future to do such a task. But again, how could you predict this because if we can predict this, then that's already happening. The same goes for DNS zone file attacks.

You mentioned talking about what could happen or what are the things that could go wrong. I do agree but how would you project that to the future? I'm trying to just understand a little bit more. The same goes for DNS misuse as a cover channel, for example. They are currently happening and there are ways to deal with these or to monitor these through traffic inspection or monitoring. But then, from a future challenge perspective, that's what I'm trying to understand better. Thank you.

ERIC OSTERWEIL: I'll take a stab at that and rather than maybe go through the three or four that you just sort of went over one at a time, maybe I'll just kind of try to push it back a little bit. So yes, a lot of these are inspired by known concerns today. A lot of those concerns, like with the vendor concern, are below ICANN purview. ICANN does not get involved at the third-level domains, generally. So if you say that there is a covert channel being used or if you say that there is a social engineering attack that's happening at the registry of a top-level domain, it's very reasonable for ICANN to wonder what that has to do with ICANN.

So our job here is to look and see do, for example, do these known attacks pose a threat in the future when people start using identifiers differently. New systems come along and they actually need to do something at a higher lee. And I don't think this list is designed to be comprehensive so it certainly isn't meant to be limiting. But in the same breath of talking about how vendor management is generally considered to be below the ICANN level, it sort of happens deeper in the tree for example, there certainly is a perspective that it related to the higher level. It could relate to ICANN later in the future. It's like well no one does X, Y, Z today.

But like Steve says, suppose there's a sudden uptake in blotching. Suppose something like name calling, which we presented in Copenhagen, takes off. That's a new use of the .bit TLD that isn't currently delegated. So how does that affect ICANN? Well, for example, that has a very big impact for identifying hijacking via social engineering because I can get in there and I can steal a second-level domain from a top-level domain and it can never ever be reclaimed because I have the private key and no one else. So that would be one way in which a known attack affects the stability at the root. So I think that's kind what the advantage of these starting points are. Denise, I see your hand up, go ahead.

DENISE MICHEL: Yeah. I think, and I'm sorry, I [inaudible] a good useful point. I think generally these areas that aren't right lines between what's happening now and what should be addressed [inaudible] concerned about future challenges and ICANN's preparations and planning. And I think as we go through the -- can you guys hear me okay?

ERIC OSTERWEIL: Oh, that's much better.

DENISE MICHEL: Okay, I think for everything on our list, we should go through it and also think about whether there is applicability to the two other subtopics, ICANN SSR and DNS SSR. And if we feel that current activities and current responsibilities of ICANN in the topics that we've listed need to be addressed, we should flag that for those other groups.

And we should also just talk through where there is overlap and I don't think it's necessarily bad. All of this is going to be coming together but I think a useful issue has been raised and for all of our issues we should also think about whether they, either instead of or in addition to, should be captured in the ICANN and DNS subtopics as well.

ERIC OSTERWEIL: Did that make sense, Mohamad? I mean, I think it makes sense but did that sort of satisfy some of your concerns?

MOHAMAD AMIN HASBINI: Yes, I do agree, and I think we'll just point out this via text and we can discuss further from there.

ERIC OSTERWEIL: Okay, sounds good. So we're coming up on the end of the call so I'm going to try and blast through this real quick. The last section that we had identified here was new dependencies. So maybe this will feel like the most futurish of the things that we've talked about so far but keeping in mind how old things are used in new ways is important. But then for example, in the future, we may want to worry about new cryptosystems and by cryptosystems I mean like cryptosystems in the mathematical sense like RSA, like Bliss.

For example, DNSSEC and how it continues to use these things in a post-quantum world. New uses for DNS is they're going to change the way we use DNS when the IoT and the new smart city fits into that and starts to evolve the ecosystem. So I think this is one of those cases that might be helpful Mohamad, just considering you're starting your write-up. It's like yeah, yeah, this is how vendors work today but tomorrow they might work this way in which case it would affect ICANN in the following way. I think that hopefully sort of makes sense.

Alternate naming systems, we touched on name coins, Steve, you mentioned DOA, that's the Digital Object Architecture, etc. -- how there may be conflicts there, how there may be issues there, etc. Censoring, loss of confidence in standards. So this one's less based on the wire but, for example, people stopped paying attention to RFCs because it's just easier to do their own thing. I think the IoT world shows that's a very distinct possibility, they invented their own thing and put it in a cloud. And adoption of systems that don't adhere standards is sort of like cloud. So Kerry-Ann, I see your hand is up.

KERRY-ANN BARRETT: Just a quick one, should there be loss of confidence in standards or less adherence to standards? Because it may not be a confidence thing, it may just be a convenience thing.

ERIC OSTERWEIL: I think that's a very fair point. I'd actually argue it's both. I mean, loss of confidence means you stop getting people going. Loss of adherence, I mean yeah you got non-standard behaviors throughout the internet.

So I would say probably both. Having been an IETF participant for many, many years, I've sort of charted the rate of new blood infusion and it seems to have a negative trajectory. Yeah, so Steve points out that it's potentially a cause and effect scenario and I think that's actually a very good characterization personally.

Okay, so that takes us through our document. You're now all officially vetted as able to speak to this document and we should be up to speed. And with two minutes left, does anybody have any comments? Maybe this is the AOB section of the call. Kerry-Ann, go ahead.

KERRY-ANN BARRETT: I had just posted a comment earlier just to make sure that is okay with me sending this to Jennifer, my notes. And then having Jennifer just send one comprehensive set of notes to the group, if everyone is okay with that.

ERIC OSTERWEIL: Any objections? No objections. Sounds great. So Denise asked if this is our standing call or if we're meeting each week or what the plan is? I don't plan on being the presenter every time, maybe ever again. I'm sure you guys will all be happy about that. We did not do a Doodle Poll for this sub-team, am I correct? I mean, a Doodle Poll for in general, I meant.

YVETTE GUIGNEAUX: Hi Eric, this is Yvette. We did a Doodle Poll for this one call. We didn't do a Doodle Poll for a recurring time. We need to figure that out on this call.

ERIC OSTERWEIL: Can I get a show of agreement, do you we believe that we should do a Doodle Poll for ongoing? Actually before we do that, let me see how many people agree -- how many people think we should do a Doodle Poll to pick a recurring time and a recurring frequency? Okay, so Kerry-Ann would like a Doodle Poll. Denise asked if this time is okay. So Amin says Doodle Poll, Kerry-Ann says Doodle Poll, Mohamad says this time is okay, and Amin says this time is okay. This time is actually a problem for me. It gets me into conflicts with a recurring meeting I have with the Dollar Day Job.

DENISE MICHEL: This is Denise. This is not an ideal time obviously as you can tell by me jumping on and off Adobe Connect, but sounds like a Doodle Poll would be best.

ERIC OSTERWEIL: As long as no one objects to a Doodle Poll, it sounds like nobody expected this was necessarily set in stone. So I will go ahead and agree, I think it would be nice to do a Doodle Poll. It sounds like this will probably be one of the times I'm there, but I won't be able to make it.

Okay, any other comments or questions? Thank you, Yvette. Yvette says she'll get the Doodle Poll out later today.

All right, great. I think we're mostly on the same page, there's a couple writing assignments in flight and I look forward to seeing you guys on the list and on the Doodle Poll. My pleasure everyone, talk to you soon.

DENISE MICHEL: Thanks, Eric. Bye-bye.

ERIC OSTERWEIL: Yeah, my pleasure. Bye!

[END OF TRANSCRIPTION]