ICANN69 | Virtual Annual General – Tech Day 2 of 2
Monday, October 19, 2020 – 09:00 to 14:00 CEST

KIMBERLY CARLSON: Hello, and welcome to ICANN69 Virtual Tech Day Part 2. My name is Kimberly Carlson, along with Kathy Schnitt. We will be your Remote Participation Managers for this session.

As a reminder to all, this call is being recorded, and recordings will be posted on the ICANN69 website shortly after the call. If at any point during the session, you have a question or comment, please use the Q&A pod found at the bottom of the Zoom window. We will not be monitoring the chat for questions.

Additionally, you can verbally ask your question using the raised hand icon, also found at the bottom of the screen. You will then be automatically placed into the speaker queue. Once called on, our techs will engage your microphone, at which time you can unmute your line.

And finally, this session, like all other ICANN activities, is governed by the ICANN expected standards of behavior.

With that, I would like to turn the floor back over to Eberhard Lisse.

EBERHARD LISSE: Thank you. Next presenter of the afternoon session, Ed Lewis will speak about DNSSEC in APTLD.

EDWARD LEWIS: All right. Hello. Actually, I'm going to talk about across the TLDs, not just APTLD. I think I sent Eberhard a preview that was APTLD-specific. I also promised not to make this boring to Eberhard, and I'll leave it up to you to decide whether I have succeeded or not. But I thought that was a challenge here.

So, I'm going to talk about a few things, take a look at how DNSSEC has been deployed across the root zone. I have a lot of slides, so I'm going to kind of go quickly through this. That should make it a little less boring, too, if I don't dwell too much on stuff. So, let me continue on.

In the last ten years, this is what the root zone has gone through in brief. I'm showing you this for one thing to show you the shape of the curve you'll see on the right-hand side. You'll see it a couple times through the presentation. Initially, when I started looking at the status that I have started, the root zone was mostly ccTLDs—the jurisdictional-based TLDs out there—and just a few generic or commercial or sponsored TLDs in the red.

You can see from 2014 to 2017, there was a huge introduction of new gTLDs. All of these had to have DNSSEC, so that sort of skews the numbers toward DNSSEC adoption those those years. And if you look closely in the latter part of this graph here, there's a slight fall off in gTLDs. Some of them have been retired and been taken out of the root zone already.

Now for the ccTLDs, I'll do some deeper diving into ccTLDs mostly because they really haven't gone through a huge change over time. They're fairly steadily growing, mostly from the IDNs. This chart is just to show you again the shape of what this is going to look like, but also these are the regions: the Asia Pacific Region is up here. These are the ICANN Meeting regions as opposed to the UN regions—and so on down through here. Europe is in the purplish down here and so on. It's one of the largest regions.

So, first I'm going to start off talking about the level of DNSSEC. Through other TLDs, DNSSEC is pretty well adopted, but there's something to look at here. [Fold means] it has a DS record. Almost means it has everything but the DS record in place. They've signed the zone; they have keys. And there are quite a few that have none right now.

There are also other states that are available to see, but they wash out in all these charts. So, let's start with some pie charts here.

You see we have about 91% of all the TLDs are signed, and they have a DS record at IANA. It's actually falling slightly as we lose some of the gTLDs that are assigned.

None, 125 of them. If I look at ccTLDs, there are 124 that are not signed. That means there's only one gTLD that remains unsigned. So, most of the work to finish off DNSSEC through the TLDs is in the ccTLDs area. There are about 11 ccTLDs that have not yet sent a DS record to IANA to finish off the job.

Over time, it looks like this. Again, on the left-hand side that's everything dominated by the new gTLDs coming in. On the right-hand side if I look at ccTLDs, this is the chart I use as a better measure of the progress of deploying DNSSEC because each ccTLD makes its own decisions. They're not required by contract to have it, and so on. So, decision making is made more individually here.

But you see that the green area here is still steadily growing despite kind of the lack of novelty of DNSSEC anymore.

This river of silver is the set of zones that have not sent a DS record, and that's been fairly constant. Some of the members of this area have been there constantly for years. They just haven't gotten the DS record put into place.

So, the next place to look at when you look at DNSSEC operation is generally the cryptographic choices that are made. Cryptography seems to be the biggest topic—what cryptographic algorithm is chosen, and also the hash algorithm.

In DNSSEC, we talk about the word security algorithm. DNSSEC's security algorithm is actually two things: it's the cryptographic—the mathematical algorithm—plus the hash algorithm. So, we combine those two into one thing.

Now in the counting here, TLD may have more than one algorithm at a time, and that's especially true when they're doing a rollover, and we'll see some of that.

So today, right now, across all the TLDs the most common algorithm is RSA/SHA-256. Number two is RSA/SHA-1_N, and that means RSA algorithm using SHA-1 as a hash but prepared for NSEC3. We had an issue with a protocol in the early years, so we made a special designation for that.

Also in this chart, not labeled, in this black wedge is RSA/SHA-1, which is the same algorithm, same hash, but for zones that do not do NSEC3.

The purple here the is the elliptic curve one that's coming on. This salmon color here is RSA/SHA-512. If I look at the ccTLDs, I see pretty much the same, but I see a larger spread of the elliptic curve; and the percentages here bear that out.

But let me go to something that I do want to dive into. I'm not going to spend much time diving into region by region because this would take too long and probably go boring at that point.

If I look at Asia Pacific, which is where I had done the slides most recently and where Eberhard got the title, you'll see that RSA/SHA-256 is by far the dominant. RSA/SHA-1 is mostly this gold and the black wedged together with a very small sliver of the—in fact, actually one count of the elliptic curve.

If I look at the European region, I see a much different picture where the RSA/SHA-256 is still dominant—a little less so—but the elliptic curve wedge here has slipped from last placed to second place. And that was 13 of the ccTLDs that would do that.

It's just interesting to see that the elliptic curve seems to have become a little bit more of a concern in Europe.

The reason for the elliptic curve, for those who aren't following this—it's a smaller signature. It uses fewer bytes in the response, so it's been favored for that reason. I'm not a cryptographer, so I really can't say whether it's stronger, but I'm sure it's stronger and newer than the RSA signature out there. But that' s not my expertise.

This slide here just summarizes what I said for those who want to see things in print.

Now the next thing I looked at here—and this is over time, what's happened. The pie charts show the current day; these are showing what's happened over time. And again, if you look at all the TLDs, I have that [sharp] rise up there just from the sheer growth. I'm not sure what this bump is for. To be truthful, I never bothered to look into that. ccTLDs, though, also the same kind of growth over time. The numbers here are different because some ccTLDs have multiple.

But this is the area I find interesting at the end here. You see a peak where the elliptic curve keys pop up, and then you see a valley start where the RSA/SHA-1_N are starting to disappear.

This is probably a—and I say hypothesis because I haven't fully investigated this, but this is where people have introduced the new keys. They added the key to their current keyset to do the rollover and then they retired the old algorithm.

Now this chart is percentages only. I only use this the one time where [actually] 100% of all the keys seen—you see again that the elliptic curve is beginning to be adopted and there's a drop off in RSA/SHA-1.

What I don't see much is a drop off in the RSA/SHA-1 without NSEC3. This went through a downturn years ago, but it really hasn't been…The long tail is continuing there. And a long tail here, mind you, is still just the TLDs out there, so we have some hope. We should get moving on that.

So, the next thing I measured—this is kind of a weird measurement. Look at the number of keys that are in the zone. This comes from the rollover period of 2017, 2018. We were concerned about the size of our responses, so we started looking around for examples of TLDs that had a lot of keys and we found a few.

One case startled us because the TLD involved had a crash which turned out not to be related to that. But ever since then, I've been looking at the average number of keys somewhere in a [inaudible] statistic. And this is the overall time, going back for 9-10 years. What I see in this chart here is that there's a lot of just movement around here. This is where the new TLDs came into place, but recently we've hit some steady plateaus at performance in this number.

If I look at the last year and a half—or year and three-quarters now—you see bit of a muddled amount of fluttering here, and then I see some more things appear. In fact, the first thing that popped up to me was I see these fairly regularly—every quarter I see this, like a

heartbeat looking thing. And it turns out, it's in here, too, I just didn't notice it until later on.

The other thing I noticed, too, was that this—like a wedding cake pattern appears here, and you see this old normal and new normal—the red horizontal line and the brownish horizontal line—show that there's been a definite drop in the overall mean number. It's actually the mathematical mean, not the mathematical average, of keys out there.

So, I was curious about this and I went through, and I did this chart at the last-minute last week. This is a chart showing the different operators out there. And I have a personal habit of not naming names unless I'm talking specifically to someone. It's not a policy of any of my employers; I've just always felt uncomfortable pointing fingers at operators when they aren't forewarned and such.

Also, this shows a bit of the aggregation of TLDs to operators. These are backend operators, not necessarily the frontend operators.

If I do this, I see a couple things. One is that this one area here which operators 151 zones—that's where that heartbeat comes from. They've been doing a quarterly roll for quite a long time. It just isn't seen in this quarter here. And that was that periodic beat out there.

The other thing you see here, the wedding cake, was contributed to by two of the bigger operators. Those that run 241 in this point here started looking like they started doing some changes to their keys. The brownish one here—208 TLDs—they definitely have also made their

changes at a slightly different time, springtime of 2020. Also, that's where the average dropped.

This operator—I know how it is. I know who these operators are. This operator has been talking about removing some of their backup keys [inaudible] online. That's what the reduction is.

And this chart here is total keys, not mean, because the means are all over the place. They don't really compare very well. The other part of this, too, is that "others" here covers many, many, many operators. In fact, most of the ccTLDs are actually sitting here because they are individual operators down there. I don't really see a very strong thing going on here. I do see like monthly heartbeats in here going on there.

One of the questions comes up. Do people change keys quarterly or monthly? In this case, you see quarterly is done by some big operators, and monthly appears down here.

So, I have a couple of charts which I consider to be not too exiting coming up, but I've seen these in other talks where NSEC3 and NSEC are two ways [inaudible] compared. NSEC3 is dominant; NSEC is below none across the Board; and that really hasn't change over time. Again, these are the same shapes you've seen before.

A little more exciting than NSEC3—because it actually matters—is the choice of the hash algorithm using the DS record. Initially there was SHA-1. That was the original one out here in the bottom, and it's in last place now—SHA-1 only.

SHA-256 came along because people were unhappy with SHA-1 doing its job right. With the RFC, they had a special clause saying, "We should use SHA-1 until it's safe to roll to SHA-256.

So, we see here in the light blue area—this bluest color here—these are the zones that have gone to the new technology that they followed to RFC, which is quite a number of years old by now.

The purple are those that are hedging their bets, made perhaps unnecessarily with SHA-1 being included—and that making the response bigger. Silver, again, they haven't entered the game, so that's fine.

But this slight salmon color here—or off-salmon, pinkish color, I guess—are the ones that remain at SHA-1 only. And these are the ones that would have problems if we totally shut off SHA-1. There's only four total; there are two that are in ccTLDs out there.

So, looking over time again, there really hasn't been a big shift in what's going on here. We do see that the 256 is growing. There seems to be a drop off here of SHA-1 plus 256. And this little river of the other color is too small to any of these changes, really. It was thicker back here, but it's getting thinner. That's good news.

So, I have here for the rest of the talk—which my timing seems to be going good for this—these are visualizations of key [inaudible]. One thing I've always wanted to do was look at how the keys are changed over time because this tells me quite a bit about what's happening in a ccTLD. And I'll show you some examples, quite a few examples, of this.

So, I'll start with the key rollover. Back in in 2017, we initiated changing the KSK for the DNS. We started out with…The old key's ID was 19036. We brought in a new key which is 20326. Unfortunately, the two numbers are kind of similar, but that was totally an accident. It's a kind of randomish thing here.

We had the key in use for the KSK. This one was in place from forever, from before the chart started—actually, since 2010—and we used it up until we made the actual roll on October 11, 2018. While we were preparing for that, we introduced the new key, and it was put in place and it was sitting side by side for all those months up until the day that it started signing.

Started signing means the signatures appeared in the zone. So, they switched from one to the other. Eventually, we revoked the old key. That's the red area out here showing that the key was taken away.

Meanwhile, while we did that, the ZSK chugged along with a key in place. Then a pre-published key appears here. The key is in operation, and then it gets retired. It sits in place for a period of about 10 days.

And you can see here that this little stepladder is very regular; and if I look at operations that have stepladders like this, I know that it's highly automated. It tells me that things are in place without people monitoring these things—not monitoring, but they're not actively changing things. It tells me what's going on in there.

So, another view of the root zoon. This is the entire root zone for the period of the data. The data does not go back to the beginning of

signing the root zone. It starts about a year or so afterwards, but it covers everything since then.

We had the KSK in use for a very long time, and this is the roll up in here—up. Meanwhile, on the other side of here, the ZSKs have been running pretty regularly; and I'll point out, for the most part, things are pretty regular.

You see this one area here where I see some more l blue than usual? That's when the key was lengthened. I believe that's when we lengthened the key. We kept the old key around longer just in case we had to roll back for any reason. So even small changes in the way we do things normally show up in these visualizations. It's kind of cool.

So, the next one here … This is a large gTLD operator out there. And again, I masked the identify of these operators because I don't want to pick on anyone for what they're doing or what it might look like they're doing.

This is one of the large gTLDs out there. The KSK has never been changed throughout those years. It may have been changed earlier before this started. The ZSK, very regular. You see a change here. That's when the key was lengthened, and the old key was kept around just for failover, in case we needed to fail back.

This is another very large gTLD operator, and they have changed their KSK. The pale color here is in operation. The dark one, I believe, is when the key is in there but not used. This shows the signature is added, so in this case there are two signatures for all time.

And over here is a color. This color, maroon, is a little hard to tell. This is when the DS record remained at the root zone beyond the key being in its zone; and it gets pulled out pretty quickly.

On the other hand, the ZSK here was pretty steadily changed pretty rapidly. This is probably a monthly basis. If I go back, this is a quarterly basis, I believe.

This is a monthly basis, and it goes back and forth, back and forth. Then for one year, it went to a six-month period; and then it went back to the monthly basis up here.

Again, in none of these things I'm showing, there were outages, but they just show how operators can change how they do things. This is yet another large gTLD operator, and you'll see them up here as ccTLD also, later, where they had gone through a very regular way of doing some work; but then they reengineered their system, apparently—and this, I don't know; I'm just guessing—and have gone to a much slower pace of key change in the last couple of years.

So, ccTLDs. These are a couple of ccTLDs that I've worked with over time. This is one that started out running 501—the automated updates—and they used an active KSKs; but they also have this other one which was revoked. There are the revoked ones here—keys that appeared in the DS record and so on. A DS record appeared without the key in the zone in these cases.

But what's interesting in this one—and this is the period of time when we had—I call—a pioneer ran the TLD. The person here in these early

years knew what they were doing; they put things together but didn't quite, apparently, pass the baton correctly to the next generation of operators who took over, and they had to recover.

In no time did this TLD have an issue, but you see things happen with their keys—moving around while they were trying to kind of regroup and figure out what was going on here. This pink one, actually, is a common signing key, something you don't see very often. This is ZSK that's signed.

The root zone also had a DS record, so it was acting as a complete key for some time for that zone, which is a good way to operate but probably was unexpected at the time. They now have started settling back in. We talked with them last year and they had settled into a new way of working.

This is another TLD. I wanted to show the key roll. Unfortunately, the title of my slides is blocked by the Zoom control bar for me. So, sorry about that.

This is a ccTLD that has been very regular. You can see their operations have been pretty smooth. Pretty much not much of a change. There seems to be a small change here. What I did was, I can recolor these charts to show me the algorithm, and this one is a ccTLD that has changed algorithms twice already.

They started out with RSA/SHA-1_N and that appeared through 2013; and then they jumped to SHA-256 and they had been there for a number of years, and then in 2019 they converted over to the elliptic

curve. They're one of the European ccTLDs that has gone and made the change.

This is yet another one. This is ccTLD that looks like a gTLD. It's the same operator, and they also changed from SHA-1. They used the RSA/SHA-1 algorithm with NSEC, and then they jumped to RSA/SHA-256 two or three years ago.

This is a ccTLD that had started DNSSEC. They started way, way, way back before the data began and they have never changed anything since. People had said that DNSSEC was not "fire and forget," but this is kind of contrary to that where it has been "fire and forget" for this TLD operator. They have outages every year, but they fix things because their key signing is also kind of…needs some looking into.

So, I have a few more to go. I'm going to kind of go through quickly.

This is another one that was "fire and forget," but they got religion in 2020 and they started growing their keys; so, they're able to do that.

Rolling keys are important because you may need to and it's good to know how to do it.

This is the TLD that launched one of my [looks]. In this period of time, they kept adding keys. It didn't seem like they knew what they were watching. Then they had a crash and they fixed things.

They also went through algorithms at the time, too, like crazy. They went from RSA/SHA-1 to SHA-1_N to 256 where they've been. But they

have recovered now, and they have been fairly steady in their operations in the last couple of years.

This is an example of a new gTLD. They started later than the period began, so [data does that].

And this is one ccTLD which has started and stopped DNSSEC. I want to remind—some people do stop things. In this case, the jurisdiction is under strife, so they probably pulled out the security because it was probably just too much to handle at the time, I'm guessing. I haven't talked to them. But they started out nicely, they had it rolling for a while; and then they stopped. If you look at the situation, you would probably understand why.

And finally, this is a gTLD that has not done DNSSEC at all and has absolutely no history to show. I wanted to leave that one as the last one there to show that we can even show those that haven't participated yet.

So, with that, I got through all the slides pretty quickly—mostly visual things to look at. I'm looking for other things that people would like to see. I'm still developing a couple things over time. It has taken some time to produce these.

And as much as I've seen examples of changes, I haven't yet used the slides, really, to tell me where to look and ask questions about what might have happened there and what kind of lessons can we share among the TLD community for improving the protocol and also the state of operations.

And with that, I will stop my talking. I'll leave the slides up, and I guess I'll open up for questions. Is that the way we want to do this?

EBERHARD LISSE: I just needed to find my unmute button and my video button. Very nice presentation. Very interesting. Let's put it like this. If I was going to ask you, with the GPG [signed] signature [inaudible], can you send me my [inaudible] data or slides? Would you be able and willing to do that as an example?

EDWARD LEWIS: Yeah, certainly.

EBERHARD LISSE: So individual ccTLD managers could get to you and say, "Can you send me?"

EDWARD LEWIS: Yes. Actually, yeah. In fact, I just went to the last slide. My e-mail address is there. Normally, in the past I've talked with people face to face when we did that; but now, if you really want me to send data about your TLD, I'm willing to generate these slides. They're easy to generate. So, yes.

I also would like, at some point, to put these up somewhere, but I haven't quite gotten to that point yet. But yes. If any operator wants to see it, send me a request.

EBERHARD LISSE: The presentation will be put up on our usual location, but I will send you an e-mail from the [registries at ATLAS] and IFO on the IANA website GPG [inaudible]. I think that's the way of communicating [inaudible] issues are concerned.

EDWARD LEWIS: Sure. I'll look for that.

EBERHARD LISSE: Alright. Any other questions? No other questions. No hands. There was something in the chat, but it was just a comment.

EDWARD LEWIS: I see a Q&A [number].

EBERHARD LISSE: In the Q&A there is a question. "Are there plans to have some kind of dashboard with these visualizations?"

EDWARD LEWIS: Plans? Yes. I'm working on…I would love to do that. I really do want these to be out there. Yes. I'm looking forward to that. I'm not sure how it's going to pop up, but I'm working towards that.

EBERHARD LISSE: I would not be very happy if, for example, my data became available to all [assembly], so this would be aggregated by content at the very least.

EDWARD LEWIS: Okay. That's a good concern to have. I'll keep that in mind. We'll try to do aggregations and so on. There are many different ways we do this, but yes.

EBERHARD LISSE: Jaap?

JAAP AKKERHUIS: Yes. Just a quick question, and—[or, actually it will be much]. I understand this work you're doing not as part of your ICANN job, but just for your own curiosity.

EDWARD LEWIS: Yeah. That's how it starts. I'm not sure if we will fold it into something, but it started out with looking at the protocol from my history with it, going back a long, long time.

EBERHARD LISSE: Any other questions? Something from [inaudible]. "Nots that it is all publicly credible data, so there is no technical privacy associated with it. It's just, you would have to do the work that Ed has done to get the data." Oh, well.

EDWARD LEWIS: Yeah. It takes time just to have all this. I do have the information going back, and the code to do this was…it just takes time to write it. I'd say it wasn't easy to write, but then again, I'm sure all of this will be—the code, at least, should be reviewed by folks at some point to see if they agree with my poor python skills.

EBERHARD LISSE: Alright. There are no other questions. Thank you very much. Nice presentation. Interesting stuff what you can research with data in the root.

Next would be Brian King. I don't see him as an attendant. [inaudible] Brian [inaudible] from donuts, and he wanted to do a roundtable about [homoglyph names]. I don't see him. If they are on the attendee list, please wave the hands. I don't really see them, so maybe we'll [inaudible] the website [inaudible] from Ed.

And then since we can't do the roundtable, we have reached, roughly, the end of our tenure and I will call upon Stephen Deerhake to close the proceeding.

STEPHEN DEERHAKE: Okay. Thank you, Eberhard. To do a quick recap on the day, we began early in the morning my time with Dr. Ajay Data's update on the state of Universal Acceptance. He gave us a comprehensive and understandable update, and my takeaway is that this important group is truly engaged on an odyssey in a true Homeric sense. They've journeyed far, but their journey for universal acceptance is certainly far, far from over.

Following Dr. Ajay's presentation, we moved on to Ali Hussein's presentation on RDAP being carried out at the University of Malaysia. Their focus on developing a toolbox for RDAP access for MATLAB, which is an important data analysis package; and also, RDAR browser utilities for Chrome, Firefox, and Opera browsers. And they're getting some assistance on this from APNIC.

We went from there into a second RDAP presentation by Alex Mayrhofer, head of Research and Development from the .at ccTLD registry which is Austria. I might note that early on in his presentation, he implicitly reminded me about how old I am, but I'm not holding it against him.

Their work on building their own RDAP servers focused on three areas which I found rather interesting. The first is that they have a need to supply access to their registry data to the Austrian SERT which is actually run within the nic.at organization.

Second, they wish to integrate access to other internally available data sources which is an interesting idea as well. And they're also investigating advanced RDAP topics. And from what I understand, this is all in the PHP, and they're making some good use of PHP frameworks. They're well along with their project, but they've got more work ahead of them.

So, after our break we resumed with a very interesting presentation by Dusan Stojicevic—and I apologize for botching the pronunciation of your surname—of Grandsy. He presented a frightening, detailed review of what can best be described as a "we're out to get you" type cyberattack against the company recently.

I personally want to thank him for stepping forward and sharing his experience with us, particularly their recovery efforts and the deficiencies they found in their disaster recovery plan.

Further, I want to thank him for the frank review of the lessons learned from this incident. His observations, I think, should be taken to heart by all of us who run online businesses, whether they be registrars or registries.

Personally, his presentation has ruined my sleep for weeks, if not months to come, but at the end of the day, I do have to thank him for that. It's got me thinking, let's put it that way.

We then moved on to Ondřej Filip's update on recent work on .cz's KNOT DNS server. Specifically, he gave us an update on their implementation of use, the newly implemented XDP feature in the

Linux kernel. And it appears from their rework of Knot that their use of XDP has given them some tremendous speed ups and associated reduction in cost, as they can achieve the same throughput with many fewer servers than prior releases.

This was followed by Natasha D'Souza's presentation/update on CIRA's work on their development of an IoT Registry concept so that you can reliably identify and secure IoT devices, whether they be dishwashers, refrigerators, or baby monitors, etc.

It looks like they've made considerable progress since we last heard from them. Still in the concept stage, and they're looking for help from the community to take it to the next level. They've got GiveHub presence, so feel free to reach out to them.

We moved on from her presentation Michael Palage to Amelia Andersdotter and regarding drops and IoT devices which was a nice follow-on into Natasha's presentation of the work that CIRA's doing.

And Amelia's focus is on what I would describe as the aviation trust framework for digital environments. They initially started focusing on drones and tagging drones so that drones could be uniquely identified and traced back to ownership, etc. It looks from their talk that they've expanded their work to human-manned aircraft as well.

And again, like CIRA's approach, there is the DNS component. There is a DNS component in their developing proposals.

And lastly, after lunch, Edward Lewis of ICANN gave us a detailed and chart-filled talk on the status of DNSSEC through the years—hash and

cryptographic mechanisms used over the years, key roll over frequency, etc. Actually, it was fascinating stuff. We have, now, sufficient data for interesting historical review on the whole concept, and interesting to see how ccTLDs in different regions were using different encryption mechanisms.

And if I understood him correctly, he's seeking input for what other things the community would like to see in the way of information and how we would like to have it presented. And hopefully soon, he will have some section of the ICANN website devoted to his work on a regular basis because I think it was pretty interesting.

And Eberhard, that's a roundup for me. I hope it was useful to everyone, and I turn the floor back over to you, sir.

EBERHARD LISSE: I must say I was also quite fascinating by a few of these presentations, and I hope that we can do Cancun number two. I actually went to Cancun, and it's a nice place—not as overrun as I thought it would be. So, I am looking forward to being allowed to travel again. I barely made it back. I cut my trip to Germany off and came back on Monday afternoon at 2 o'clock when they locked up the country at midnight.

I hope we can do Cancun and see each other there; otherwise, we'll do it virtually again.

Alright. Have a nice afternoon, evening, night, or whatever it is. And thank you very much to ICANN staff, in particular Kim and Kathy, but also the technicians that are listed here; Dustin [inaudible].

Thank you very much for supporting us. Good-bye.

[END OF TRANSCRIPTION]