PANAMA – ccNSO: Members Meeting Day 2 (1 of 4)
Wednesday, June 27, 2018 – 09:00 to 10:15 EST
ICANN62 | Panama City, Panama

KATRINA SATAKI: Good morning dear ccTLD's and Friends present in the room. I see some are still celebrating, as yesterday we had an excellent, wonderful, ccTLD community cocktail and I'd like to start today by thanking, wholeheartedly thanking all those who sponsored, who made that event possible, those are DOT BR, DNIC, still celebrating, American Samoa, Steven, not in the room but he was in the room. Dot BI, BI Nick, Transversal, thank you! Dot NZ, and VeriSign, thank you very much, David.

Thank you very much for making this possible, and I also would like to extend my thanks to Kim who worked day and night to make sure that we get all great offers and a great place. I just saw Steven Posing there, but he left. He went to GAC room apparently. So, thank you very much, thanks everyone, of course to the excellent participants, the cocktail of course without you it also would have been a little bit boring. Thank you very much, and with that, let's start the second day of our CSNO members meeting, thank you, have a nice day.

JACQUES LATOUR: All right, thank you. I'm Jacques Latour, I'm with Dot CA, so today we have a panel on natural disaster, disaster recovery and business continuity planning. This is the outcome from the last meeting in Puerto Rico where there was an interest raised by the community to do something around this topic. Today's panel, we'll go through what we think we heard from the community. We'll go to a couple of slides to revisit, we'll go to our proposed strategy for TLD ops to address this, and then we'll look at a presentation from Pablo from the Dot PR, with adjust to impact, so you'll be on.

Then we're going to look at different aspects of disaster recovery, business continuity, so Irwin is going to go through their plan overview, Dot CA will go through our plan overview, and the same thing with Regis. You'll see that we have a different approach, and it's not a one shoe fits all solution, which is the challenge that we need to address because the work that we need to do needs to work for most of us, not just a particular ccTLD, and then we expect at the end to be more interactive and then get your feedback, and your feedback is going to decide whether or not we continue on doing something with DR. With this, I'll give it to Regis.

REGIS MASSE: Thank you, Jacques. I am Régis Massé from .FR, I'm a TLD Ops standing committee member, and this morning we will focus on the new projects we want to work on with the community about disaster and recovery plan and natural disaster. As you may know, TLD Ops group is not just a mailing list, a security mailing list from the community; we try now to deliver stuff to help ccTLD's and the first delivery was the DDoS mitigation playbook, I will pass very quick on this because I think most of you in the room know about that, so the goal of this playbook was to help ccTLD's how to prepare and to face with a DDoS attack, and it was the result of two workshops in Copenhagen and in Abu Dhabi, and now the playbook is delivered in the final version, and it was, I hope it will be useful for our CC's.

Now that the first delivery is over, we are to find another project to work on with the group and the community, so after the Puerto Rico ICANN meeting, we heard the presentation of Pablo from [inaudible] the presentation of Yuro from Japan, and we think that it would be a new interesting subject to work on, on natural disaster and what is the impact for our ccTLD's. So, In Puerto Rico, as you know, and Pablo will talk about that, was recently hit by one of the strongest hurricanes in recent history. There was no problem for Dot PR, because they didn't have any impact because of recovery plans in place, it's very important.

They have a plan, and the plan was played and they have no impact for the community and for the registrants.

After that there was a survey conducted at the beginning of the year to collect information of type of disaster and emergencies the ccTLD's have faced over the last years, and if we summarize the survey, the result of the survey is public, so you can read it. If you take some highlights from that, we see that four TLD's report recent natural disasters since the beginning of the year, so it's important. 50% of respondents who experienced disaster in the organization is to make that the time taken to recover operation was under 6 hours, that is from our point of view very good. When there is a disaster, bringing back up older systems are no doubt a factor in less than 6 hours is very few I think.

Organization with large domain names, more than 15 hundred are generally set up to perform remote disaster recovery if needed, and 78% of ccTLD's consider the organization either prepared or very prepared for disaster or emergency. If we see in this survey, people think they are ready, but are they really ready if there is a disaster recovery? If there is a natural disaster, didn't plan of course, and what will be the impact for the CC's?

If you look at this map just very quickly, we will see that there were natural disasters in Caribbean, in Asian Pacific area, and there was power failure too. It's the most important natural

disaster we have this year in the survey, and if you look at the survey, you will see that there are other kinds of disasters that may occur. Network for example, the things like that. But we want here to focus on the natural disasters for this workshop.

About the major root causes, today we have raised some kind of typologies; earthquakes, hurricanes, cyclones, tornados, volcano eruptions, maybe in the future a moon collision from space, I don't know, but these major root causes are different and what is important here is to notice that where in the world the natural disaster occurs are not the same for the CC's, and I think one of the aims of the workshop in the community is to share experiences from what they have and what they face when we speak about natural disaster. Now I will give the floor to Pablo who will focus on what happened in Puerto Rico.

PATRICIO POBLETE: Pablo Rodriguez from NIC Chile. Is there any reason to focus on just natural disaster and exclude man-made disasters like terrorist attacks or cyber attacks or things of that sort? Actually, the power outage that you showed in Chile was a truck driver running into a high-voltage tower, I don't know if that qualifies as a natural disaster, but it was a disaster anyway, because it left half the city with no power for many hours.

PABLO RODRIGUEZ: I am sorry, Patricio, I will address a little bit of that. As a result of what we have been doing in LACTLD, but indeed, you are absolutely correct; it's not only natural disasters, it's also man-made disasters.

JACQUES LATOUR: So, you're stealing the pitch but towards the end it's general disaster recovery, and general business continuity to address all eventualities, so yes.

PABLO RODRIGUEZ: Good morning all, my name is Pablo Rodriguez, from the ccTLD Dot PR Puerto Rico, just next door. It is an honor to be with all of you here, and my presentation this morning, for those of you who were in San Juan will be very familiar, although I have added a few other things that I consider that are relevant and important to this discussion.

I will go very quickly over some of the slides, and I would like to make a disclosure statement; I am not a meteorologist, nor am I an expert in atmospheric sciences, but one thing that is quite evident and scholarly literature supports, undisputedly is that the concentration of CO2 gasses in the atmosphere continue to

trap solar energy, thus warming the oceans, increasingly warming the oceans, making them more acidic, pretty much in the same way that when you add CO2 to your carbonated soda will make it bubble and makes it acidic. We know this because our oceans are getting warmer, our coral reefs continue to die in very massive proportions, which are alarming to those of us who live in this particular area of the world, and we continue to see an increasing number of hurricanes.

The hurricane season for the Caribbean region began in June 1st, so we are already in the middle of hurricane season in the Caribbean. It has been forecast that we will have a number between 13 and 15 storms this year, of which between 3 and 5 will be category 3 or better. At the condition that are many of the Islands, we don't need a category 3 or anything, all we need is a good tropical storm, not even a hurricane, and it will wreak havoc in our region.

I would like to quickly go over hurricane Maria, what happened at the time.

[VIDEO PLAYING 00:13:00 – 00:13:52]

A couple of things that I'd like to bring to your attention. This occurred on September 20th. Until this date, September 20th of 2017, until this day, we have over 20 thousand families without

electricity in Puerto Rico; nine months later. Over one hundred thousand people without electricity, so to assume that you have a natural disaster and you will recuperate very quickly is a fallacy.

Second, as registry operators we need to be sensitive and be aware that these things occur. One point that I'd like to bring to you is that natural disasters do not occur independently of each other, but before I go onto that I'd like to point out to you, look at Puerto Rico before the hurricane; actually, on satellite images Puerto Rico was the most lighted Island in the Caribbean. After the hurricane, that's what Puerto Rico looked like after a recuperation, a significant recuperation was made. As you saw in the previous video, it was totally black; there was no light.

Out of 16 hundred Telecom Towers, we lost more than 14 hundred of them. It was a very dire situation. No electricity, and if there is no electricity, there is no pumping, no pumps to pump water from lower levels to higher levels, there were no treatment water plants, so now water treatment plants were discharging polluted water into the rivers, therefore you cannot go to the river to drink water. On and on, and everything gets complicated very, very quickly.

This is an example of what I was talking about, and I would like to highlight that these cables, they weight tons, literally tons,

and you need helicopters to raise those cables. Once you have a tower, we can discuss other alternatives that were used, such as what we call now COWS; Cell on Wheels that were used. Moving on very quickly, what did the PR do to remain operational? We knew it was a matter of time that we were going to get hit by a hurricane. I mean, it's a matter of statistics, right? They continue to come by, at some point one of them is bound to hit you.

We had two call locations, we had one at critical hub, and we have a larger one at AT&T. We had bunkers there, we had fuel for a number of days, we had power cells, we had all of our racks were there and mirrored servers at critical hub as well. Guess what? After the hurricane passed, there was a tremendous shortage of fuel, no diesel fuel. Critical hub was down in three days. On the third day, they called me and said, "You know what? We are running out of fuel, please tell us if you want to come and shut down your servers or you want to let them go, they will shut down by themselves." That is a horrific situation. When you are told that you are going down, there's nothing you can do about it, you are going down.

Thankfully, we had a second mirror at AT&T and we were able to maintain our DNS. In addition to that, we also had DNS Anycast technology, and we had Anycast technology in Germany, and we

had Anycast technology with PCH, and we intend to also very soon have Anycast technology with LACTLD, and that was part of the strategies that we used to remain, to maintain our DNS, so our DNS was never lost.

As Regis mentioned, the hurricanes, they're natural disasters that continue to occur. Depending on the region, it will be hurricanes, cyclones, earthquakes, tsunamis, but the one thing that I want to- if there is something, a couple of things that I want to take with you from this session. One is; natural disasters in general and disasters in general, and natural disasters in particular, sometimes occur in multiples. It's not necessarily that we had one hurricane, no, you will get hit by one hurricane, no electricity, no water, there's a number of disasters one behind the other.

For example, when I made an interjection while we were watching the video, I said, "Look at the date." Puerto Rico was hit on September 20th, a hurricane hit Puerto Rico on September 20th, but on September 19th, the day before, guess what? There was an earthquake in Mexico.

[VIDEO PLAYING 00:19:37 – 00:20:13]

Again, you're looking at a region that gets hit, is extremely vulnerable to natural disasters, and just within 24 hours, Mexico

has an earthquake, and within less than 24 hours Puerto Rico gets a hurricane. And then you get this; the volcano fire in Guatemala. To me, that's unheard of. I've never seen anything like that.

[VIDEO PLAYING 00:20:46-00:20:50]

I'm so happy to report that the ccTLD in Guatemala was unaffected, and they were perfectly fine, and we have evidence here because Alejandra is here. I called her, and the first thing I said, "Ale, please tell me, how are you? What is going on?" I mean, that was really, really impressive to us. That's right next door to us.

And this, this is what really got us, this is what made us very aware in 2011.

[VIDEO PLAYING 00:21:24 – 00:22:33]

That's what I looked like after the hurricane. It's hard. You come out after a disaster like that, and you don't recognize your own landscape. I had no idea where I was. I looked around and I looked at my father-in-law and I said, "Where the hell are we? I don't recognize this landscape," and that's what it looked like. It's total chaos, total disorientation. What happened? What happened?

As you saw, it's not just one disaster, it's that you will get hit from all sides, from all possible- and it's Murphy's Law. If there is anything that can go wrong will go wrong, and it will hit you and it will hit you very quickly. You will have no time to recuperate. There is no time to reflect, there is no time to think; you need to get prepared right away. You need to be prepared.

When that happened, we thought that it was important that if a disaster occurs, regardless of natural or man-made occurs, on the other side of the world from our perspective, imagine; Japan is on the other side of the world as far as I'm concerned, from my perspective that's the end of the world. Am I responsible for what happens in Japan? The answer is yes. We feel that we are. We are responsible for our brothers, and so what we did, immediately, is that we went to our databases and we began to search for domain name users from those particular regions.

We looked for Japan, Thailand and so on, and we found quite a bit of Japanese companies that had domain names with us. Only a few little domain names, Sony, Nikon, Cannon, Fuji, Honda, Acura, Toyota, honestly, am I going to let them expire because they didn't report to me? Because they didn't pay their registration fee? I mean, honestly? Immediately what we did is that we extended the expiration date for as long as it takes. I'm

pretty sure that Sony is good for the money, they will pay me whenever they have the time.

We did extend that, but seriously speaking; the one point that I would like to bring to all of you is that when you find out that there is a natural disaster anywhere in the world, the least we could do is look in our databases and see if we have someone from that region, and if we do, let's protect their domain names. Do not let them get expired. Continuing on, as we mentioned, we immediately looked in our databases and we went into a renewal process for all of those domain names.

When it happened to us, we immediately followed a search of all the domain names that were registered, whose country of origin were in the path of the two hurricanes that you heard. Puerto Rico was not only hit by Maria, Maria was the one that made landfall, but we had hurricane Irma pass by 8 days earlier, only 35 miles away. If we're talking about a giant atmospheric event of hundreds and hundreds of miles that passed us by 35 miles away from you, the hurricane, the tropical storm forces that will pass by you are just enough to destroy your infrastructure. You didn't need to get a hurricane.

This is something, and Patricio, this is for you; when we talk about these type of events, this is from a Harvard Business Review Report that was recently published in May, and it shows

that in 2017 out of 106 attacks, 70% of them were repelled, but nevertheless, 32 of them were successful and penetrated. In 2018, 2032 attacks and 87% were repelled. We're getting better at repelling, but look at the penetration rate, it remains pretty much the same. More money equals to more protection; not necessarily. The average cost per crime per company, millions of dollars in 2013 was 7.2 million dollars, and by 2017 it was 11.7 million dollars, an increase of 62% and penetrations continue to take on.

There are four ways to look at what is the cost of cyber attacks on us. Average cost of cyber crime per company, how much does it cost each company? What is the annualized cost of cyber crime per sector, and in this time, I'm asking about the LAC region, because I recently presented this in the LACTLD, to the LACTLD community, and we need to generate our own statistics, therefore, we need to start capturing statistical data on that. But what is the cost on detection, on containment, on recovery, investigation, incident management, expose response, or business disruption, information of loss, revenue loss, equipment damages and other costs. What is it that these people are after? There are many, many different industrial sectors there, they have one thing in common, and the one thing they have in common is personal information, credit card information, that's what they're after. Over and over again. Yes,

there is industrial espionage and a couple of other things, but mainly it's all about the money.

What I would like, the other thing that I would like for you to take with you is that we should start a dialog, we should start a serious dialog and see how we can institutionalize, how can we make it a standard, a best practice that when such a disaster, whether natural or man-made occurs, regardless of how far it is in the world according to your perspective, we should do something about it. We should rally to help each other out. These are some of the references, I take it that this will be available, please seek out these articles. Thank you very much for your attention and thank you for giving me this opportunity.

JACQUES LATOUR: Thank you Pablo. Next slide. All right, so what we saw is natural disasters mostly, so I think the TLD Ops committee, when we looked at this, we need to implement, we need to look at disaster recovery for systems and application and look at business continuity for the people and to ensure they can continue their work, and we need to figure out where TLD Ops is going to focus their work in there.

If you look at it, Pablo covered most of this, but you need to have a disaster recovery plan for your DNS infrastructure, so Anycast

helps with that, but over a certain period of time your zone might go stale, so you need to have plans to keep it up to date. The registry system, having a disaster recovery plan for that, being able to have the redundancy and having different architecture for that, this is something that can be standardized, but you need to have plans for your registry and your systems and the data.

You also need your IT infrastructure, and you can keep on working, you need computers, you need network, you need access from your corporate infrastructure to the registry or the DNS, so you need tools to work, and you need plans for that.

BCP on its own is the business continuity, so what do you do when there's a disaster, where do people meet, what is their corporate plan, people aspect is different than the system aspect. There is disaster recovery, business continuity, is very, very broad. TLD Ops can't cover, we can't do everything for everybody. We need to be specific on the piece of work that we're going to do in the short term.

Based on the result from the ccTLD, it's circled there, so there is a need, there are ccTLD's that are somewhat prepared, or not prepared to handle a disaster or business continuity, and this is an area perhaps that we could focus on is, how do we increase a maturity from the smaller ccTLD or the ones that are not ready

to show a plan on what they need to do to be more ready. That's an area that we can look at.

You'll see that natural disaster is the third cause of disaster. Cyber attack is the number one that has impact on the registry, so business continuity, if you look at this from this point of view, it's more important to have better, based on the number of incidents, it's probably fair to assume that the smaller ccTLD's that are not prepared should be more prepared to handle a cyber security attack. If we're going to start somewhere, then we should be handled to support a disaster. I'm not saying it's not important, but based on the requirement, that's probably an area that we should look at.

Disaster recovery, plans for your registry, your DNS, in case of cyber-attacks. TLD Ops already did some work here last year because we built a DDoS mitigation book. If your disaster is getting a DDoS attack, then we already have a playbook that you can look at and implement the work in there to be more prepared to handle a DDoS attack.

I think we covered a little bit of that, but we haven't addressed a compromised system.

PABLO RODRIGUEZ: Jacques, and the audience, I would like to bring to your attention that indeed cyber attacks are more prevalent, and the frequency is greater than any other of the disasters. When a natural disaster occurs, everything else happens. Net power failure, network failure, software failure, people are concerned about their lives and that of their families, so everything is disrupted, and it seems that they continue increasingly, therefore, if you are going to make preparations to protect yourself against cyber-attack, also make sure that that is solid enough against a natural disaster.

JACQUES LATOUR: Thanks. Based on that, I'd like feedback from the room. This is important. Where do you want us to focus, more on compromise registry disaster, you get somebody hacks into your system and what do you do to recover? Or, you want to focus on business continuity planning and have some plans to help, so we can't do everything, we need feedback from you. I'm not going to say this, but the best answer is for us to do nothing because we're lazy. The next step is, we do something, which means we do work, and where do you want us to focus on?

PABLO RODRIGUEZ: And the options are disaster recovery or…?

JACQUES LATOUR: If you look at TLD Ops, what we did is we have a contact repository, the contacts are security persons inside the ccTLD, so I think it's more natural for TLD Ops to focus on security, a compromised system for example, because we have the right people in the mailing list than to focus on building a business continuity plan for your business, but most of the TLD Ops people, committee, or CSO or CIO's and we know how to address business continuity, but it's not exactly in line with what TLD Ops was meant to do.

The kind of information we exchange on TLD Ops, is, "Watch out for this malware, it might impact you." That's the information that we share on the list.

UNKNOWN SPEAKER: If the room stays quiet I can talk from here. One suggestion would be to start to work as a more general or generic playbook for disaster response and crisis management response, because how you respond to a crisis will be, at the higher level similar wherever the disaster is. You have to have your crisis management team, how do you communicate, we have our offices ready to meet, how do you meet, do we have the numbers, who else do you talk to? Your registrars, your

registrants, your [inaudible] providers, all those things are probably similar no matter what the disaster is.

That would be one way to attack the issue, to start by a generic playbook that you can just fill in as a CC for your specific operations and then we have more time after that, we can start adding some scenarios more specific, like a natural disaster or a cyber-attack, but start with the generic response of the things you just need to be prepared, once a disaster hits you don't need to think about these things, they're written down, you just act right away and you get on your feet right away.

JACQUES LATOUR: Yes, you're allowed to ask questions, just get up, go to the mic, the mic is there, it's the little thing on top of the post, you talk in it, and we can all hear you.

UNKNOWN SPEAKER: I wasn't sure if it was time for asking questions. So, I represent Dot PK ccTLD, we just got our application in for being a ccNSO member, so we'll be glad to become a member, thank you. One of the things that I would like to bring your attention to is not from a physical infrastructure point of view, from more of a policy point of view. One of the things that we have done for disaster recovery is to actually have mirror sites across the

world, and we are a private TLD, we are still not managed by the government and obviously whenever there is a government and there is a private TLD there is sort of a rocky relationship back and forth.

Another thing that we, I guess if we can use the word "harassed", is that whenever we tell them that we have mirror sites and we have all of this, for obviously our better service for the community, they come back and say, "This is a breach of national security, this is our data, national data, if you place it in the US, and Europe, then what happens if they grab the servers and take all the data away?" I was just curious as to what the experience has been for other ccTLD's and is there sort of generic best practices or a good response that we could give back to the government in that case, that would be appreciated, thank you.

JACQUES LATOUR: Thank you. We can respond to that after.

PABLO RODRIGUEZ: I just wanted to comment that I really like the idea of the playbook; I think that is very common sense to begin with, write things down, have some kind of playbook. We don't have much to think about, we know exactly how to react, and as you said, it

gives us a platform from where to start and then we can start building on top of that, good idea, I really like it.

JACQUES LATOUR: Together, most of the bigger ccTLD we have well-documented DCP plan, we have disaster recovery plans for all aspects, it's all documented, so this is an example from the Dot CA critical event protocol; this is the initiation of an event. So, something happened, staff, somebody discovered something happened, they don't know what, the building is gone, the DNS don't work, the registry is dead or been compromised or whatever. Anything that happens at CERA, DR related, BCP related, goes through this process.

So, something happens, it goes to a manager, we look at the event, we assess, it goes to the senior level management team, and this is, we have a protocol to define if it's a critical event or not, and then all of this is documented in our BCP plan, but this is typically how if somebody sees something, how does it get engaged to go here?

Then, we have an activation plan and like Pablo said, a certain event can activate one or more plans in parallel, so it could be something that you need business continuity, you need a new office to work in, and you also need to recovery your registry and

bring it back online, and maybe other services need to be turned on, but you need to do all these plans in parallel, you need to have enough resources, depending on the event, so it's a bit complicated.

Maybe what you're saying is we can start to have a high-level plan with the high-level bullet and over time keep adding. Would that be useful, something like this? Yes?

I guess the easy part. Going to the mic is too far, but we have cards. Maybe we do green card, we should build a high-level plan, if you're interested and see where it goes?

There's two things we can look at- okay. Based on the outcome of this, I think there's two choices; either we develop or generate a response plan to start addressing a disaster or a business continuity issue, TLD Op focuses on a security-related compromise, very specific plan, like one of those plans, at the bottom, IT continuity plan, a registry continuity plan or a cyber security compromise plan.

I'll ask for either one, and then what we can do in Barcelona, on the Sunday we could have a workshop and either simulate a disaster and then work through the process all together, and then we figure out with flip boards what are the key things we need to do for each one of these things and then we can build

the playbook out of that and then if you're there then we have tons of experience in the room, we can make a lot of good stickers. But, we need to know where the focus is, because we can't do everything.

Feedback on the business, plan, the business continuity, or how do we do that? Cyber security plan in red, BCP in green? Barcelona, a session in Barcelona, yes/no? All right. So, standard BCP plan. And then in cyber security compromise type of disaster, like a recovery plan. And we have zero minutes left. Good, thank you.

Pablo is joining TLD Ops, right?

PABLO RODRIGUEZ: Thank you, that's what I heard.

DEBBIE MONAHAN: Good morning everyone and welcome to the session. We will get to interrogate, sorry, talk to and ask questions of our ccNSO board members. And our special ccNSO board member, so this is an interactive session where basically it is you that is going to be asking questions, but to kick things off, I'd like to ask each of them a question related to a topic that Jordan is actually going

to be chairing and talking about later on this morning, which is WICC stream 2 and the CCWG WICC stream 2.

And while we are, the order might be a little bit wrong because you haven't heard from Jordan, but when you're listening to Jordan later on this morning, you can take into account the responses we received to my question of; we'd like to hear, well, I'd like to hear, I'm sure the others would too, what the board think of the recommendations that are coming out of that WICC stream too, and any comments that you may have for us to consider when we're hearing from Jordan later on this morning?

CHRIS DISSPAIN: Good morning everybody, thank you all for coming out. The CCWG final report hasn't come to the board yet, obviously, it comes to you first and then it will come to us, although the board is briefed on it, and the board has been interacting with the chairs of the CCWG to talk about things that the board might find difficult in the report, and to see if we can find ways through that. I think we've reached a point now where we're probably, whilst I suspect the board as a whole, and certainly individual members of the board might find some of the recommendations challenging, difficult, or maybe even be totally against them, I think we've reached a point with the report where there's at least a reasonable chance that the board will look on it and say,

"I think this is okay and we can pass it on." We can pass it on, sorry Liz, I apologize, I'm speaking directly to you.

I'm happy to speak personally, I think although we have been told that it's impossible for us to speak personally because you're always assume we're speaking on behalf of the board, which is of course utter nonsense but anyway. Speaking personally, I have a couple of things that I'm uncomfortable with. I'll accept them, but I'm uncomfortable with. I think, and I will tell you one of those and that is that I think this concept of a five or six-person panel in respect to the ombudsman to sit and advise the ombudsman is probably not the most brilliant suggestion on the planet, but we can live with it and that will be okay as long as it's structured properly.

I don't want to pre-empt what anybody else says, and I don't want to pre-empt what the board does, but I do think it would be fair to say that there has been a really good interface between the chairs and the board. I think it's been excellently well managed by the chairs, especially given that the chairs themselves have changed throughout the process, and so therefore there have been, suddenly you find yourself dealing with somebody else, but nonetheless, I think the chairs have done an exceptionally good job of -- except of course for Jordan. They've done an exceptionally good job of managing it, and it's

been a very, very difficult process and I'm pleased that I've come to an end of it. At least, I hope we have, once we get the report, thanks.

BECKY BURR: I agree with that, and I think there was a time when then package of ombudsman proposals were troubling, very troubling. I think that the co-chairs have worked with us and listened to our concerns about that, and we've got things into a manageable situation. I just want to talk a little bit about the unthankful task that's sort of hanging out there with work stream 2, which is the IRPIOT, which David Macauley has been working tirelessly on. It's incredibly important that we get a set of processes for the new IRP panel in place, and I think we're very close to doing that.

There's one issue that's going to go back out for community support on this, or technical, only the things that lawyers would love. But the hard work of figuring out how to select a panel and see the panel and get it, that's coming up, that's critically important, that was the reformed independent review process with a standing panel, was one of the cornerstones of the accountability work, and it's unfortunately getting us a long time to get there but I want to thank David for really

unappreciated work and urge all of you guys to start getting engaged in this so that we can wrap it up.

MIKE SILBER: I think it's difficult coming at the end of two such eudicots of speakers, but I think the point is that it doesn't move with quite the same urgency that we saw in Work Stream 1 and that's understandable, but I think we've seen some pretty solid work coming out. I am less polite in terms of the ombudsman recommendations. To me, they're just ill-conceived, but if that's really what the community wants, well, then waste money on that you can find five people to travel around the world doing random arbitrary things instead of actually focusing on mission. But, I do recognize it, that a strong ombud is important to an organization of this nature, I just don't see how that panel achieves that. But, we'll move on. We have a lot of irrelevance in this organization, this will be just one of many.

CHRIS DISSPAIN: Mike, as usual, subtle, tactful, and not telling us what he really thinks. I just wanted to pick up on what Becky said on the IOT thing, IOP stuff, and totally acknowledging David's extraordinary work, but I think it's an example of a danger that occurs in this organization and in the multi-stakeholder model. One of the

issues with the IOP working group is that is that people have kind of been there and they've kind of gone, and there's any left with the last man standing. And the last man standing is generally the noisiest and generally the one with the most strident opinions and generally the one that ends up influencing the process.

Because nobody else is paying attention, you end up with this really difficult thing and you end up getting stuff, which if you actually thought about it, you probably wouldn't agree with, and that is a real challenge. It's a real challenge in all sorts of things. I don't think it happened too much in the CCWG. It happened a little bit in some of the working groups, and if you look at some of the people that were the loudest voices at the very early stages of the CCWG, the first stage, they've disappeared because their job is done, and so they came in, they flew in to lobby, they got what they wanted and then they've left.

That is actually an issue for this model that we need to be careful about, which is that we don't just become, a single issue takes off. In the case of the IOP, the struggle is at least in part to do with a drop off in people paying attention to it, and therefore the person who's paying the most attention ends up winning the day, if I can put it that way, it's not necessarily "winning." So, this is something that we need to be really careful about and

something we need to watch for the future as we do more and more things in a cross-community way. It's the same within your individual SO and AC, but less, it happens less because there tend to be more people who prepare to hang on in there. Thanks.

MIKE SILBER: If I can add to that, I think that's where the reviews come through, and that's where reviews are really important. Up until now, the IRP reviews have really- I don't think that they have looked at trimming irrelevance from this organization, and I'd really encourage all of the people who have put so much effort into this process going forward to look at some of the structures and to look at some of the little whirlpools that we've created, because we felt it was absolutely vital at the time, and just to every so often take stock and say, "Do we really need this additional process? Is this actually adding any value?"

And yes, some of them, so the empowered community may not be used for twenty years, but it's vital that it's there. But, there are other mechanisms that were created because there seemed to be a need at the time, and when after three or five years they're not being used, then please, I employ you, I may not be around, but just look at trimming them, don't leave things there because it's tradition.

DEBBIE MONAHAN: Great, thank you all. Now, any other questions from anybody else please? Or, Jordan, do you have any comment that you want to say if I haven't had it from the board? Come on, surely, I know we had the drinks last night, any questions?

NIGEL ROBERTS: As not quite a board member yet, I've got a question for Mike; have you got any comments about the last nine years you'd like to share with us?

MIKE SILBER: It looks like Jordan has something he wants to say, is that on the previous topic?

JORDAN CARTER: No, it's just a different question.

MIKE SILBER: So, let me answer. My years have flown by, this is a really interesting organization and I really appreciate the faith showed by the ccNSO in appointing me for three successful terms, even though I didn't particularly want the last one, I do appreciate the

faith you showed by nobody volunteering to stand against me in the third round, so I suppose I had to do it.

But, it's been an incredible learning experience, I think you guys are all very special, but also think that you operate in one of the sanest parts of this organization. I think some of you have had that experience going through the CCWG, those of you who've gotten involved in gTLD's who are involved in other parts of the organization or have expanded your vision to other parts of the organization, have seen just how nuts it can be out there.

The critical thing for me is that this organization of Country Code Managers is a really unique community because you operate well, you cooperate well, you don't see quite the same interocean politics that happen elsewhere where you work together one day and you stab the person in the back the next, so please try and retain that.

At the same time, recognizing that you're in an increasingly competitive environment where you're dealing with competition from outside, from inside, from changes in the way that DNS has been used, and you need to keep alert, and I think ICANN has a responsibility to help focus its attention on some of that, and I think you need to be insisting that the organization does that, not just for the loudest commercial voices, but also for ccTLD.

JORDAN CARTER: This question is kind of, it might be a bit difficult for you to answer but I'll try anyway. The way that ICANN has handled the GDPR stuff over the past couple of years has almost been a case study of how not to do it, late to the plate, rushing things through and so on and so on. And, you might disagree with that characterization but I'll stand by it until I die. How are you going to make sure that this doesn't happen again?

In other words, what do you think ICANN needs to do to be able to, this on the gestation period in 2012, it was passed in 2016, here we are in 2018 still getting ready to deal with it. How do we make sure that the organization is better at noticing things that are happening and responding to it?

MIKE SILBER: Let me go first from a non-GDPR perspective, Becky is obviously a lot more focused and a lot more knowledgeable in the specifics of that issue, but in terms of the general approach. While I don't fully agree with your characterization, there are certainly elements that resonate with me, and I think logically it's a question of an inward-looking focus that we've experienced up until now. A belief that our model and approach is sacrosanct and therefore nothing else can touch us.

I know we have one enemy and that is IGO's and the [inaudible] process and that's all we need to worry about, and I think that led to an incredibly myopic view of other policy initiatives, and certainly as a board, the one thing we've told org to do is to pull their head out their rear end, and that they actually need to focus more broadly on multiple initiatives, not the very narrowly-focused existential defense that we've focused on.

Some people need an enemy that we can fight against, and so we had a single enemy, which wasn't our enemy and I don't think is our enemy, but we had one adversary. Instead of actually looking at the broader landscape and saying we need to look at all the initiatives, they may be very friendly initiatives but they will have an impact. I think that the current leadership that we have, from a board perspective and also our choice of CEO was very important in looking for somebody who had a broader perspective, who wasn't one-dimensional, who wasn't defensive, who wasn't looking for an adversary to fight against but actually more broad-ranging in terms of things that could impact the organization, so I'm pretty comfortable that that tunnel vision that we previously had has been removed.

BECKY BURR: I am not going to dispute the proposition that ICANN could have done it better, but I do think it's worth taking a look at what we

were doing between 2014 and 2016 and what was going on in this organization and a degree to which there was bandwidth to think about the specifics of GDPR, so I can tell you that we finished the transition and at the board workshop in January of 2017, we devoted a significant amount of time to GDPR. Having said that, this issue of WHOIS has been on the table since 1998 and we have not been able to reach an accommodation to the data protection concerns that have been raised throughout this.

My opinion, that's because a group of, a significant group of people had what they wanted in the form of open access and their position was, "We're not changing it, try and make us," and there wasn't a process absent a crisis like an external law that gave ICANN a compliance hook. So, yes, Mike is right about the organization has to be more aware of the environment, the legal and regulatory environment, that's been made loud and clear.

But, the other thing is, we have a problem in the policy development process, and we have a problem, we've seen it in some of the Workstream 2 working groups where there are rewards for holding out, so I think one of our focuses coming up should be to think about whether we have the policy development processes properly aligned, whether we're thinking about consensus in the right way, whether there is a

way to align incentives to bring people to the table with a commitment to get work done in a timely fashion.

As I said, I'm not going to dispute the fact that it could have been done better, but it could not have been done through the policy, we've demonstrated over and over and over again, that we needed this external forcing event with a compliance hook so that ICANN could actually make some decisions.

CHRIS DISSPAIN: I agree with Becky, and I want to add just a little bit of color to the sort of bold statement that it could have been done better, and it's not to justify, but simply to remind us all that it's never as simple as; this thing happened and you should have handled it better. Some of the color includes the fact that in, and I cannot remember what year it was but I will check, I think it was about 2013, in that we got a letter from the Article 29 working group and we had had letters from them before, and we went to the GAC with a letter from the Article 29 working group, and at the time in the GAC there was a very senior official from the European commission who was their representative, and I cannot remember her name but again I will check it, and her response to us, and it's in the transcript was, "The Article 29 group has no authority whatsoever, we're in charge, you should ignore them." I mean, I'm paraphrasing slightly, but that was in

effect what it said, and we wrote back and said, "Thank you very much indeed for your letter, it's great to hear from you, go away." So, there's that.

There's what Becky said about the transition. There's the fact that frankly, and again, speaking entirely personally, there's an appalling piece of legislation that has absolutely no sense, makes no sense, and is based on a premise that doesn't work from a lawyer's point of view, which is, "We'll make a broad brush philosophical statement and you figure out what it means." As far as I'm concerned, that is totally unacceptable, and it shouldn't happen, but it does.

But that's just my opinion, but Jordan, you're quite right, and as Mike said, we've put in place a whole series of steps to ensure that it doesn't happen again and its part of our strategic plan for the next five years is a system to ensure that we know what's coming down the pipe and so on and so forth, but let's be really clear; this is not over. Even if we had solved the GDPR problem, in other words, the registries and the registrars have got a way of dealing with it and WHOIS is working fine, it's not over, and it's not over because there are other governments who will pass legislation that directly conflicts with GDPR. It is not over.

BECKY BURR: Just one final word, I do privacy all day every day for my day job, and anybody who tells you that they're 100% GDPR compliant in any kind of complex environment is lying. Or, delusional.

DAVID MCAULAY: Thank you, David Mcaulay is my name, with Verisign, and Becky thank you for the very kind remarks. I just wanted to pick up on the IRP implementation team and the fact that we have actually one more rule for public comment. It was out for public comment before amongst a body of rules, it's now discreetly by itself, and the question is; should there be an overall limitation, time limitation on a party's ability to bring a claim at IRP and is there some reasonable overall cap that should be decided upon.

It's an important question because we're trying in IRP to also build a body of president, so all I want to mention is; that is out there in the dreaded summertime in the northern hemisphere, but it's a very discreet question it's not a great amount of, it won't require a great amount of work I wouldn't think, it's open for public comment until August the 10th and I would encourage folks to take a look.

Let me also say as a long-time, from the beginning participant in the CCWG and accountability, I think you are absolutely spot-on on complimenting the leadership, all five co-chairs from the

beginning as well as staff led by Bernie who I think is in the room. They've done an excellent job. The advisory panel for the ombudsman is working its way through, it's a bit of an odd duck, I too wonder how it got there, but all in all, very good work, so thanks to them, thank you.

DEBBIE MONAHAN: Any other questions?

LIZ WILLIAM: Liz William speaking, slightly different question. Yesterday in the sessions we had, we had a lot of notes up about how many members we have in the ccNSO who doesn't attend, who is not active, where they don't come from, any suggestions for how, as a group, we can encourage more participation and we can encourage more ccTLD managers to feel that the work of the ccNSO is valuable and relevant?

MIKE SILBER: For starters, I hope that list was GDPR compliant.

CHRIS DISSPAIN: So, the straight answer to your question Liz is actually find an issue that galvanizes people or find a common enemy. But, in

essence, this has always been a thing with the ccNSO, there's a reason for it to be here, it's very important, you will all be delighted to hear that I gave Brad White an interview for the history project which apparently is going to go up before Barcelona and talked about how the ccNSO started and why it started, and what kept us all coming back.

But, the truth of the matter is, if there isn't work to do that people want to do, then all you can do is keep having the discussions and provide benefits. Peter, you know, because of with Center, how do you get people involved in Center? It's no different, so the best answer you're going to get Liz is to go to people like Peter and Leona and ask them about the Center and APTLD and how they keep their people involved there.

MIKE SILBER: Just having been in your previous session, and compliments to Jacques and the panel, because having been involved in the management and operation of the ccTLD previously, the ability, especially with smaller ccTLD's to learn from experience, to gain access to templates, to benefit from the learning given that most of us in this room operate in some sort of public benefit mode. There are only a few ccTLD's that are still privately held.

I think that that public benefit expense beyond just national public benefit, but also to the global community so I'm really impressed and I would encourage you to look beyond just the business continuity processes but start looking at sharing best practice and other processes, putting templates up.

I think even if you don't get people at meetings, you certainly bums on seats is a very good indicator, but visits to templates, views, downloads, when you start seeing, again, not just to pick on that one but it's fresh in mind, if you start seeing your template business continuity plan popping up on ccTLD manager's websites all over the place, adopted for local usage, well then you know that you've succeeded; it doesn't matter how many people were in the room at a meeting.

DEBBIE MONAHAN: Right, thank you all. We've heard from the three current existing board members, but of course to my left is our incoming board member, and so I'd like to ask Nigel, I was going to be rude, but I've decided not to, to actually talk us through how you plan to transition from being a ccNSO councilor to an effective representative for us on the ICANN board?

NIGEL ROBERTS: Thank you. It's actually quite a coincidence that I'm sitting on your left, it's just where there was a spare seat. I guess it must look like the other current board members and as the new one, so I'm feeling a bit like the new boy.

CHRIS DISSPAIN: When you've been shipped, you can come to this side.

NIGEL ROBERTS: I'm feeling a bit like the new boy at the first day at school. As you know, there was an election. It seems like it was a very long time ago, perhaps it was. I just want to say again, thank you for your confidence in me. There's been a little bit of confusion about people I've spoken to about when I'll take up the role. A number of people have said to me, "What? You're not already on?" In fact, it's not in fact until the end of the next ICANN meeting. Technically, it's at the end of ICANN's general meeting when new and incoming board members take up their role.

So, what's happened since the election all those weeks and months ago? First of all, council and then this magic department, the ECA have some formalities to do, and that took a little while, and they did that. Of course, my notes have just gone off the screen. And, when they completed their formalities,

ICANN staff reached out to me and said, "I'm here to help, I'm from ICANN, I'm here to help."

I got an invitation to attend the board workshop that's going to be taking place in September, as an observer, so that will be before I take office, and as we saw from the last AGM, the board has adopted a new procedure of integrating and involving incoming board members in the AGM and the activities there to a greater extent so I expect to be taking part in that.

I had a meeting with Shireen a couple of days ago over an hour and it was extremely welcoming, extremely informative. I learned that there are a number of issues that are facing the board, which directly in fact affect ccTLD's quite considerably, and guess what? It's not all about GDPR, there's some serious stuff coming that ccTLD's are going to have to pay attention to shortly.

There's been a ccNSO councilor election in the meantime and I'm extremely pleased to note that my replacement, Giovanni, take a bow, is taking office I believe at the end of today's council meeting, which is my last official act. If you have any other questions please talk to me directly or yell at me now and thank you again.

DEBBIE MONAHAN: Coffee time, and I'm pretty sure that by the look of most people you could do with coffee. I would like to thank, you've been up here at the table with me for your efforts and hard work, and the demands on the board are very high and demanding, so thank you. And, Nigel, enjoy every minute of it. Thank you all, please come back here for 10:30 for the start of the next session, thank you.

[END OF TRANSCRIPTION]