MONTREAL – ccNSO: Members Meeting Day 1 (1 of 5)
Tuesday, November 5, 2019 – 09:00 to 10:15 EDT
ICANN66 | Montréal, Canada

KATRINA SATAKI: Good morning, ladies and gentlemen. Good morning ccNSO members, non-members, our friends, and colleagues from other communities. In preparation for this meeting, we actually have a couple of things we'd like to highlight. One thing was that … I looked for some Canadian proverbs and one of the proverbs says that if you talk about the sun, you will see her beams. I looked outside today. I think Canadians are overly optimistic. I think we can talk about the sun the whole day but it won't be helpful. However, I hope that by this evening – and Alejandra will you more information about this evening – at least it's not going to rain.

Another thing that's Canadian … Well, one of the Canadians said without Montreal, Canada would be hopeless. I don't know why. But one thing I want to say, without Montreal perhaps ccNSO wouldn't have existed because Montreal is the birthplace of the ccNSO. And I know that some people were here in Montreal when the ccNSO was born. May I ask those two stand up and wave to the community? Don't be shy. Yes! Thank you very much. I think it was well done.

Again, I don't know about Montreal, but I know that without DotCA and CIRA, Canada would be hopeless. And may I give the floor to Byron Holland, the CEO of CIRA, our host here in Montreal. Byron?

BYRON HOLLAND: Thank you, Katrina, and welcome friends and colleagues to Montreal to the fourth Canadian ICANN meeting. It was really interesting to see how many people were at that 2003 Montreal meeting that really was the birthplace of the ccNSO. So, great to have those folks who have that institutional memory, that knowledge and that commitment to this community because that's quite a commitment. But also, of course, welcome to all the folks who have joined us on that journey ever since and to the newcomers.

In that period, most of us have shared a similar path but very different journeys along that path. And I wanted to take the opportunity to share a little bit of what CIRA's path has been over those years, to talk a little bit about where we've been, but probably more importantly about where we're heading and how we see ourselves as a ccTLD operator fitting into the broader ecosystem. And I'm sure some of it will be familiar to you but hopefully some of it also gives you pause for thought or reflection.

So, CIRA, our vision is to – I don't know if we can get rid of the text box in the middle of the presentation. Our vision is not 47447703. Thank you.

So, at CIRA our vision is to be a world-class domain name registry that's recognized and valued by both the Canadian Internet ecosystem and DotCA registrants, as well as the broader Internet ecosystem. And we really do that primarily by being an effective steward at what we consider public resource, the DotCA. And taking a leadership role certainly in the Canadian ecosystem, but to the extent that we can, in the broader international domain as well.

And every time we do the things that we do, it's always viewed through that primary lens of, "How do we build a better online Canada?" That's the first question we ask ourselves when we engage in the activities where the services or the international fora that we participate in. How is this building a better online Canada?

So, we are back here in Montreal and Montreal is a wonderful city. CIRA is based in Ottawa about 200 kilometers down the road. So, this is, without a doubt, the closest ICANN meeting to home that I will ever go to and I'm pretty sure the only one I will actually get to drive to.

But Montreal is a great city and I really encourage you to take the opportunity, if you can, to get out and see a bit of Montreal. It is, of course, home to what many people know as the Canadian dish Poutine which you can see on the left. It really tastes better than it looks, so while you're in Montreal, you really should have Poutine.

It's also home, of course, to the Montreal Canadians, one of the original six hockey teams in the NHL and, without a doubt, the most storied team in the NHL and of course Canada is very much a hockey nation, so Montreal to some degree is the epicenter or the shrine of hockey in Canada.

But to this community, I think it's probably even more interesting to note that the world's first search engine was developed her in Montreal in the late 80s and went into production in 1990. And it was a search engine called Archie and came out of McGill University's computer science department. And they built it to help them find programs on the Internet but it was actually the first search engine that the Internet had seen.

It's also around the same time that I'd kind of like to start our journey today back in the late 80s and the birth of DotCA. Don't worry, I'm not going to walk you through every step. We'll just touch on a few highlights.

Over the past year, my Board and myself and my team have been engaged in developing the next five-year plan for CIRA. So, that's also given us a lot of opportunity to reflect on where we've come from as we think about where we want to go and all of the challenges and opportunities facing CIRA and DotCA but I would say also our broader community. You don't have to read it all.

And some people say nothing happens at ICANN but if you make the timeline long enough, a whole lot of stuff looks like it happens on a timeline. The boxes in red – and of course you don't need to read all the details – are really DotCA specific and the gray, the broader Internet ecosystem.

But over roughly the last 30 years, or just over that, DotCA and certainly our community have seen a remarkable amount of change and have engaged in driving – we, as this community – in driving that change.

So, back in antiquity in our industry, through the 80s and 90s, DotCA was delegated in 1987 to a man named John Demco who was essentially the founder of DotCA and John Postel personally delegated it to our John Demco in '87. And it was, like many of us in this room, based out of an academic institution, University of British Columbia in Vancouver on the west coast.

It was run there for 13 years by a merry band of volunteers. So, you can imagine – and I don't think this is a dissimilar story to many of the stories in this room but it was run by John Demco who led the compute facilities in UBC and a group of computer science students and others at that time.

The first DotCA domain name was registered by the University of Prince Edward Island, 5500 kilometers away from UBC on the other coast. Ironically, even though UBC was the home of DotCA, it didn't register its own name until the next day and therefore is not the first DotCA registered.

but those years, of course, were many of the foundational years in terms of policy development and the organization's development and our industry's development. Not just, of course, in Canada but in the Internet ecosystem globally, including the creation of the Internet Society and InterNIC, one of ICANN's predecessors in the management of DNS and through the emergence of other key organizations in what we would probably now call Internet governance but that wasn't really a term in those days.

But, of course, 1988 also saw the advent of something we don't love which was the first worm, if anybody here remembers back to '88 and the Morris Worm.

In what I would call the middle ages, the second decade of our development, that's when we really saw the Internet as we are starting to know it take shape in the late 90s with the advent of

Google in ’97 and the commercialization of the Internet really getting into full swing. And that’s of course when we saw the US government get involved in handing off the operations of the Internet and the formation of ICANN in ’98. And coincidentally – or maybe not coincidentally – that is when John Demco and UBC initiated the process to hand off the CA registry to a more community-oriented fit-for-purpose organization. And in ’98, that started in Canada, and in 2000, CIRA took over the registry, in December 2000.

It’s also when, I think, during that period, the initial WSIS happened and that ultimately led to the IGF, the well-loved IGF that many of us continue to participate in until this day.

But it’s in December 2000 that CIRA took over the management of DotCA and at that time it had 60,000 names registered. So, that’s what CIRA took over from UBC.

By 2008, actually when I started, we had just under one million domain names. So, over those roughly ten years, the initial ten years of CIRA we went from 60,000 to one million.

And in 2008, as an interesting footnote, given the times we live in today, we introduced full privacy in our WHOIS for individual registrants a decade before anybody had heard the acronym GDPR.

So, in what I would consider the current times or modern times of the Internet, we – and I say that we collectively as well as CIRA continue to evolve in the industry – we've seen, of course, massive expansion of the root with all the new gTLDs, and over this time period, another billion or so users come on to the Internet.

But with all of this growth and with the wonder that is the Internet have come a whole range of issues that we've had to face and deal with, too, and certainly trust I would put among the top of the list.

And to my mind, while there were certainly events prior, 2013 and Snowden really kicked off a series of questions that we have to ask ourselves about trust on the Internet, our role in the Internet, and where it's heading in terms of security, stability, and ultimately trust.

It also led to responses in other organizations like the IETF with new protocols, certainly including something like DoH which is a top-of-mind issue these days.

And I think all of these issues still continue to have a wide and profound effect on our community. And it's not just the technical issues, which of course as the technical operators we think of as our remit or being affected by, but it's also the fact that governments and other actors are becoming more and more attuned to the issues of the day and issues that we consider really relevant to our community.

And it's not just the GDPR but GDPR symbolizing government's increasing interest in our community or the functions that our community is engaged in. And how do we respond and grapple with that increased interest?

One of the top-of-mind issues at this meeting is what's being referred to as DNS abuse, but quite frankly, I would challenge that notion. Words matter. When we talking about DNS abuse in the context of the way it's being talked about today, is it DNS abuse or is it content abuse on the DNS? And words matter and they will very much continue to matter going forward in our discussions with government. And I think it's important for this community to be one of the educators and communicators in this issue in particular. Thank you. But it is, obviously, something absolutely critical to us and near and dear to our hearts and words will matter on this issue.

And that brings us, I think, to today because we are, by definition, technical experts. Technical organizations and technical experts. And we have a really important role in helping our governments, helping other communities understand the importance of these issues and what those words mean. And I think it's imperative that our organizations continue to be involved in these discussions, if not lead them, and certainly CIRA believes that and, as part of that, just last year we helped relaunch the Canadian IGF where some of these issues can be discussed in meaningful ways with broad community. And we also participate very actively with other organizations in the ecosystem, be they ICANN, IETF, IGF, with our regional registries and the more.

But domain names will always be the critical part of our business. However, we certainly, as we've looked at the future, engaged in other areas other than just domain names.

And this just gives a brief, very high-level overview of some of the activities that we're engaged in beyond domain names. Clearly, DotCA is job one, will always be job one. But we've expanded our remit into cybersecurity services, Anycast, firewalls, and the like, as well as registry services. We built out a new platform where DotCA is customer number one, of course, but it's a multi-tenant environment and we have a number of other registries on that platform.

We're very involved, as I've already touched on, in the global Internet ecosystem and Internet governance. In Canada, we try to contribute back to the community in material ways, be it our fostering and catalytic activities of Internet exchange points across Canada, among other activities and sharing that with other colleagues in the room. And learning, of course, from other colleagues in the room.

We also have a very robust community investment program where we give back in terms of grants to the community for worthy Internet-related activities and we typically fund about 25 projects to the tune of $1.2 to $1.5 million a year and have done that for the last six years.

But I think all of these things are, to some degree, a reflection of this room, of this broad ecosystem because I know many of us are doing many of these things. Not all the same, some different, some more, some less – but as a broad reflection of the space that ccTLDs occupy.

I think while I've touched on some of the milestones of the past for CIRA and for the ecosystem, more importantly is the future for CIRA and for this community, because I think, as ccTLD operators and certainly as CIRA, it's incumbent upon us to really be thinking about how do we continue to develop and build the Internet, a better Internet, for tomorrow.

Back in 2003 or certainly prior to that, the Internet envisioned by those early luminaries, some of whom you saw stand up here today and their peers from before that, it's probably not the Internet they quite envisioned at that time. And whether it's misinformation, privacy issues, security, access, governance structures, etc., there are issues that we need to deal with as technical operators, even if many of them are purely policy driven.

Last year, every year, CIRA conducts considerable first-person research and last year we focused on Canadian's perceptions of the Internet from a security perspective. And there's a few things that I thought I'd share with you from a Canadian perspective. The significant majority, almost 90%, of Canadians are very concerned about cybersecurity attacks on their organization and the impact on personal data. 80% are very concerned about security threats posed by IoT devices. 60% admitted to being taken in by misinformation and fake news. 60% of Canadians admit they've already been duped by misinformation. That has potential profound impacts on our society and open democracies. All societies, but in my case, open democracies.

They understand the Internet is a powerful force for good – and it is, of course. We wouldn't be here if we didn't believe that. But, there are many issues that I think even as technical operators, we must stand up and face.

In order to preserve the environment of innovation and trust that we have developed, as ccTLD operators, as network operators, as actors in the Internet governance space, I think we have a really important role in this future, in the future of the Internet, to maintain and improve the Internet for years to come, in spite of its maturation, our maturation as an industry, the things that we worried about like apps and platforms and new gTLDs. I believe there is a huge amount of opportunity for our ecosystem.

At CIRA, our vision is to build a better online Canada. In ICANN, they talk about one world, one Internet. And it struck me that the ccNSO doesn't, per se, have something like that. It's certainly referenced in documents the notion of for and by ccTLDs, which I think is a really interesting starting point. But as I consider the future for CIRA and our role in the ecosystem, I put it out to this community.

As we face all of these challenge and opportunities as the ccNSO, is there an opportunity for us to share that common vision in our work towards building a better Internet? I'll leave you with that. Thank you very much. Welcome to Montreal and we'll see you tonight.

KATRINA SATAKI: Thank you very much. I'm pleased to see that more and more people are joining us today. Please note that there are still quite a few chairs in front, so if you want to be closer to the event, please come to the first row.

Thank you very much, Byron. Byron gave us some bits of information about tonight but we still have a full day today, full day tomorrow. I'll give the floor to Alejandra to walk us through the agenda and the most interesting bits, although everything is interesting. But Alejandra will provide some update. Alejandra?

BYRON HOLLAND: I'm just going to jump in for one more second because I did forget to mention, all things Canadian, I'm not sure if you know that our national coffee chain and donut chain is Tim Horton's. So, as we go to the coffee break, we have tried to give you a little bit of Canadian and we will be providing the national food which is Tim Horton's Timbits, so on your way out, feel free to grab a Timbit on your way to coffee. We'll have them at the back.

KATRINA SATAKI: Excellent. Thank you very much.

ALEJANDRA REYNOSO: Hello. Thank you very much. And the clicker is here. So, good morning, everyone. Today, I am going to walk you through what we are doing today. Maybe not. Let's wait a little bit for that. Sometimes, systems fail us. Should I try? Not yet? Let me check. Oh. Well, some technical difficulties there.

Anyway, you can see some of the faces of the meeting Program Committee. If not, may I please ask the ones that are here, if you can please stand up, committee members, so they can see you. Thank you very much. Thank you.

The purpose of this slide was for you to see your faces and to see who we are, just in case you have any questions or you have some suggestions or any comments you may want to share with us. Please, approach us. We are very open to anything you want to say.

This is our ccNSO secretariat. They are the ones who make almost everything here in ccNSO possible. So, thank you very much for your hard work. Also, please feel free to approach them if you cannot find us. There is also their email if you have any questions. Please know their faces and come to them just in case you have any questions. I will try to put the next slide. Thank you.

So, do we have anyone who is the first time coming to a ccNSO meeting or that may be has been quite a while and you are coming back? Please stand up. Don't be shy. We want to see you. We want to know you. Oh, good crowd! Welcome, welcome! Thank you very much.

For you to know, we have this quick guide to the ccNSO. There's printed ones here in the front of the room that you can reach me if you want a copy. We have it online, of course, too. But just in case you want to get it back home with you and have some notes, we have that. We also have an ICANNLearn course that you can access and learn more a bit of the ccNSO. So, please. We have information for you.

Also, for everyone, these are your quick links. The presentation will be available to you. The quickest access to all presentations here is in the full ICANN schedule. The URL is quite easy. There is also the agenda that you have printed on the tables. But those who are not yet at a table, you can have it online.

There are also session summaries. So, if, for example it's been a while since you've been here and you want to catch on the topics that are being discussed, please look at the summaries. And if you want to get notified about sessions of the ccNSO, you can subscribe to our Google calendar. There is also the Wiki for anymore information on working groups and committees. So, this is super useful information. Please use it. Thank you very much.

So, for today, photos have some issues. We will start the day with the DNS and the Internet of Things chaired by Katrina. But you all know her. She's right in front of you. The yellow one. Then we will have accountability and transparency review that Demi will chair. We will have the briefing of ccNSO workshops by Barbara. And a very, very interesting session regarding the candidates for the ICANN Board questions and answers led by Byron. So, stay tuned.

We will have one of our most preferred sessions. It's ccTLD news. This is where we share our experiences, where we say what we have done. Good practices and things to learn from experience. This will be chaired by Gudrun and by Barbara.

Also, our last session of the day will be the ccNSO Organizational Review that Nick will be chairing. This one in particular is very important for us because, as you know, we have been reviewed. We have some recommendation and we need to go through them. And just for a teaser, we have a Council workshop and we will discuss that in that meeting. In the workshop, we ask these questions to ourselves like how we see ourselves, how we think the community sees us and how they might actually see us. So, stay until the end of the day to see what happens then.

After that, we will have a very wonderful evening. It's Canada Night. Thank you very much to CIRA for the event. Please note that this is invitation only, so if you have already RSVP'd through the link, that's excellent. And we will walk there. It's very close. Maybe 10-minute walk. So, please go and enjoy. It will be an amazing night.

So, that's for today. But tomorrow we continue. So, please be minded that even though we will have an awesome time tonight, it is very important to wake up in time for meetings. We start at 9:00. It will be very nice to start like this with a full room. We have some important sessions, such as the IANA naming function session led by Abdalla. Then we will have a ccNSO appointed ICANN board member session. You can see them there. It's Chris and Nigel, so come to have a chat with them. Then we will pause a little bit here. We will move to the plenary session on DNS abuse. This is in the main room. This is after coffee break. So, coffee break we go to that room. We stay there for the session and then we come back at 1:30 here.

We will have our policy session led by Patricio. Then Q&A with candidates for the ccNSO Council Biyi. And we end our sessions here with a very, very interesting panel on ccTLD perspectives on Internet governance. So, this will be led by Young-eum. It will be an interactive session, so we are expecting you to participate.

After that, there will be a ccNSO Council meeting in room 518. You're all welcome to join us but we will move from the room because this layout does not help us through our discussions.

And even though we have two member meeting days, there are still some relevant sessions for us on Thursday. Here are the ones. In room 514-A, we will have an IDN ccTLD policy review and next steps and there will be also the meetings program committee session. You are more than welcome to join us.

And in the main rom, there are several ICANN general sessions such as the ICANN public board member, another plenary session regarding the evolution of the multi-stakeholder model, Q&A with ICANN organization executive team and the second public forum. So, stay tuned to that.

but before I wrap up I want to share with you some important information. We all here are speaking in English but not all of us are native speakers in English, such as myself. You can tell by my accent. So, please, when you are here in front of us or when you go to the microphones, please try to speak a little bit slower than usual so everybody can hear and understand what you are saying.

Also, please, before anything, say who you are. For example, I would say, "I'm Alejandra Reynoso. I'm from the GT and this is my question," or my comment. Please do so mostly because we have remote participants and they want to know who is on the microphone. Maybe they cannot see you on the cameras.

Regarding the microphones, we have two microphones. One on each aisle. So, feel free to stand up, walk a little bit and go to the microphone if you want to have a comment. If you don't feel like that's for you, you can join us in remote participation, in Zoom room. Here you can type your questions if you don't feel like you want to speak. Those get priority, by the way. So, if you need something to go through really quick, please put it in the chat there and our secretariat will be glad to read them for you. So, please participate. We want to hear what you have to say.

Also, keep calm. This is a very friendly environment but do please be on time. We want to start every session on time, so be mindful of the time allocated to you, which by the way, I don't know how I'm doing with that. Right on time. Good.

After we finish our two member meeting days, a survey will be circulated by email. Your feedback is our most precious income of opportunity to improve. So, please, when you receive it fill it and let us know what you think about the sessions, the layout, the content, which topics you would like to see in our next meeting. We want to hear from you because this is for us. So, please, tomorrow it will be available to you, so fill it.

We are not only seeing each other and hearing from each other in face-to-face meetings. We have lots of ways to get in touch with the community. There's social media. There's website days and newsletters that you can subscribe to you if you want to get news on ccNSO and what are the latest events. There's also the ccNSO secretariat email if you have a specific question. There's also, again, the Google calendar for any events that are posting there for you to be aware of.

With that, welcome to the ccNSO.

KATRINA SATAKI: Thank you very much, Alejandra. I hope that you noted the most interesting sessions for you. Those who are too shy to come and look for chairs, here we have chairs in front, so please don't stand there. We still have chairs here. We have chairs there, too, next to this guy who he's not as dangerous as he looks. He is very nice, actually. You! So, please. Welcome, Keith! And here we still have chairs. Please, please join us. Thank you very much.

Now we can move to the next agenda item and that's DNS and the Internet of Things. As you heard earlier today, Byron already said that … Well, he started talking about shaping the future of the Internet. This is probably one of the ways how the ccTLDs around the world … I'll give the floor to Jacques and Cristian.

CRISTIAN HESSELMAN: Good morning, all. My name is Cristian Hesselman. I'm with SIDN, the registry operator for the DotNL domain and I'm also with the Security and Stability Advisory Committee. So is Jacques on my right-hand side over there. He's with DotCA as well.

Today we'll be talking about the DNS and the IoT and the opportunities, risks, and challenges that this introduces from a security and stability perspective. We'll also be trying to discuss a few ccTLD specific items and opportunities there.

Today's goal is basically threefold. One is to provide an overview of the interplay between two ecosystems, which is the IoT ecosystem and the DNS ecosystem which I think most of you are pretty well aware of. And in particular, discuss the opportunities, risks, and challenges that the interaction between these two ecosystems introduce.

Also, we'll provide a few examples of ccTLDs activities in this space, in particular done by DotNL and DotCA. We also have DotIT in the room somewhere and they are also active in this field.

The goal of the session is basically to trigger and facilitate dialogue within the ccTLD community which is also the objective of the document that Jacques and I co-authored which is the SSAC 105, a document released by the Security and Stability Advisory Committee. Our goal there is to trigger and facilitate dialogue within the broader ICANN community. So, in this case, it's for the ccTLD community, specifically.

The motivation for having this session is basically that there's overlapping work between SSAC 105, the document that I just talked about, and the work that we're doing at various ccTLDs and perhaps we could also consider the IoT a strategic issue, maybe similar to the DoH discussion.

So, the Internet of Things. We basically used the definition that ISOC provided back in 2015 which is an Internet application that extends network connectivity, computing capability to objects, devices, sensors, and items not ordinarily considered to be computers.

We believe that there a couple of key differences between traditional applications and the Internet of Things. The first one is that the Internet of Things, other than traditional applications like email and web browsing, interact with the physical world and they do this through different types of sensors that collect information about people, about physical environments, process that information usually on a cloud service somewhere and then act upon the physical world through actuators. And this is something that takes place in the background of our daily lives.

So, usually we're not aware of those interactions and we usually are not involved in them either. That's what ISOC called passive interaction. That's different than writing an email or clicking on a link somewhere which we would consider active interaction.

So, projections are that the IoT will eventually consist of some 20 to 30 billion different devices and that they will be widely [inaudible] in terms of operating systems, network connectivity, and that sort of thing.

Another thing that might also differentiate the IoT from traditional applications, the lifetime of IoT devices will typically be much longer because they might be integrated into physical structures, and as a result, they will operate unattended very often and they will perhaps need to operate for decades rather than for years in the order of years.

So, to sum up, we think that the IoT promises a safer, smarter and more sustainable society, but IoT security – you saw that one coming – is a major challenge that we need to address.

Within the SSAC, the thing … And also with, let's say, this also applies to several ccTLD operators active in the field of IT security, the [inaudible] botnet of late 2016 was basically a wake-up call when a botnet of around 400,000 to 600,000 infected IoT devices attacked the DIN operator which resulted in outages of various popular services, such as Twitter and Spotify. The same botnet also attacked other types of infrastructures such as the [inaudible] which is an ISP in Germany.

So, for those who don't know, and IoT-powered DDoS attack involves many infected IoT devices sending traffic to one target simultaneously, thereby denying the target the service that it needs to provide, hence the term Denial of Service Attack.

So, this is the model that we're using within the SSAC when it comes to the IoT and the DNS. As I mentioned before, we consider it two interacting and co-evolving ecosystems. And there is an example in the graph that you are seeing here, so I'm just going to discuss part of it because the rest is too much information.

So, we think of the IoT in terms of IoT deployment and a deployment is basically a combination of three things. One, IoT devices. So, these are the sensors and actuators that interact with your physical space. Services that process this information to enable the devices to provide their functions. And network connectivity to connect these two together.

so, there's an example in the top. There are two deployments in this example. Let's go through the deployment number one, So, that's DP1. It's basically a smart watch collecting all kinds of different – with different types of sensors collecting information about a user. That information is being sent. So, that's D1 in the graph. That information is being sent to S1 which is a service that operates somewhere in the data center and that decides, based on various types of inputs, such as maybe your body movement or voice commands or that sort of things, if it should send a command to an online door lock to open the door lock. So, there is two types of interactions here with your physical environment. The watch sensing information and the actuate of the door lock, the three acting upon your physical environment.

So, this is typically how IoT devices work. There have been many studies that confirm that IoT devices work this way using a backend service. Mostly, end users are unaware of that.

Also, what people are not aware of is that these IoT devices use the DNS to locate the services. So, that's the black box in the middle. D1 and D3 in this example, they interact with the DNS to discover the IP address of S1 in this specific example and S1 as any other service on the Internet registers with the DNS so that it can be discovered by clients.

So, that's basically how the IoT and the DNS ecosystems interact. And much of what you're seeing is hidden under, let's say, behind the IoT devices themselves.

So, the study that we carried out within the SSAC, we looked at three things. We looked at opportunities. We looked at risks and we looked at challenges. So, I'm not going to go through every one, through all of them here. I'm going to refer you to SSAC 105 document for the details. We also have a blog floating around somewhere. But what's important is that the opportunities for … there are opportunities for the DNS because the DNS is a globally distributed infrastructure that's ubiquitously available.

So, this means that if you get DNSSEC, for example – DNSSEC validation. If we can get that to work all over the planet, then we can protect IoT devices from, let's say, being rerouted or redirected to malicious [end] services. So, the devices in a previous example, they connected to S1, but they might be a malicious version of it as one prime that the device would then send personal data to or that it would receive instructions from. And with DNSSEC, you can avoid that. So, that's one possibility.

Another possibility would be to encrypt the DNS information between IoT devices and the resolver that they use. This is important because sometimes IoT devices release information about themselves in the domain name that they're looking up.

So, for example, there's examples where they have … So, there's an example in the text over there, [inaudible] .hello.is. So, you can see that this is a Sense device, which is a brand. So, there is information that IoT devices release about themselves which you can hide using, let's say, DoH, for example. So, DoH is DNS over HTTP which is encryption.

So, in addition to the opportunities, we also spotted a few risks. One is what we call DNS unfriendly programming. So, IoT developers that are basically unaware of how the DNS operates and what the effects are, if they use it in a certain way. So there have been a few examples where apps, for instance, use the DNS in a naïve way, and as a result, ISPs got kind of DDoS by these devices and there were only 700 in this specific example, so imagine that this scales up to millions of IoT devices all trying to use the DNS in a DNS unfriendly way. I'm trying to stay away from the technical details a little bit.

So, the other risks are the DDoS attacks, but that's something we already talked about before at the beginning of this presentation. Then there is DDoS amplification. So, we have around 23 to 25 million open resolvers on the Internet and they can be used to amplify DDoS attacks, and as a result, the DDoS attacks that IoT botnets launched can be multiplied by a factor of 29 through 64, so you can imagine that this can, let's say, have quite some effects on infrastructure operators.

Then, we also have provided a few challenges. Again, not going through all of them. So, one of them is to develop a DNS security library for IoT devices so that IoT software developers can link them into their software, and as a result, make DNSSEC validation, as an example, available to IoT firmware, for instance.

Another one would be to handle IoT-powered DDoS attacks more collaboratively, for instance, by exchanging information on DDoS attacks such as IoT-powered DDoS attacks between different infrastructure operators, and as a result, become more prepared for DDoS attacks that are coming from the IoT.

So, there's a bunch of other challenges that we envisioned. So, for instance, explainable security. How do you explain to people who buy IoT devices in their local store, their local shop, how secure these devices are and what they should be looking at for. And another thing would be to have edge IoT security systems that detect anomalies early on in [inaudible] networks, and as a result, clip off potential DDoS attacks as soon as they start. We'll be talking about that a little bit more later on.

So, then, we have two, a few, examples of the DNS and IoT work at DotCA. Jacques?

JACQUES LATOUR: Hello. My name is Jacques Latour. I'm the CTO/CSO at CIRA and I'm te lead of CIRA Labs and I'm going to talk about a couple of initiatives that we're working on CIRA relating to IoT device.

The first one, I think in my view, the most exciting one, is this summer we got engaged with an organization in Ottawa called L-SPARK and we joined their IoT accelerator program on secure IoT. So, we got into that program at the beginning of the year, this summer, and we were not really sure what to expect because we went in with another project which our home gateway.

What we discovered throughout that project is that mobile IoT device, which is an IoT device that only has a SIM card which supports 5G. So, 5G is a SIM card connection on an IoT device. We discovered that there is no framework around managing that.

So, as we got in the project, we discovered that a domain name is very similar to a 5G IoT device in that, a domain name, you can delegate it from one registrant. You can point it to one site, like the name server. You can point to one provider or another. You can transfer the domain from one registrar to another. The registrant, the ownership can be transferred to people. So, that's a domain name that we live in.

And the IoT device, the mobile IoT device, it's the same thing. The ownership, like a generic parking meter IoT device, the ownership can be the City of Ottawa to the City of Gatineau. You can point it to connect to one cloud provider or another cloud provider and then you need a registry in the backend to manage a mobile IoT.

So, in the last six months, we basically developed a prototype to replicate a secure IoT registry that interfaced between cloud provider and mobile operator and generic IoT device 5G.

So, that would be a 5G IoT registry where we interface with different parties and we enable the connectivity between IoT device. It's a bit complex how it works, but two weeks ago, we spent entire week at the Mobile World Congress Conference in LA and we presented this to a bunch of big carriers, big mobile operators to cloud provider, to IoT manufacturer and IoT cloud provide and the solution, actually the concept, is feasible and the prototype that we built actually works.

So, today, we can have an IoT device that only has a 5G card. We can write directly on the SIM card the credential and the contact information where the IoT device has to connect.

So, just like changing nameserver, we can change where IoT device connects on the cloud and we create certificate and the whole thing actually works. So, CIRA is going to join the [Geo Summit] and we're going to start doing the technical specification or this.

But I think opportunity is obviously CIRA, if this thing works and CIRA can run it globally, we will, but I doubt. But I think it's an opportunity for ccTLDs as well to run this in their own country, so I'm not sure how the deployment scope. But certainly, the government has an interest in making sure IoT deployment is done securely within their country. So, more to come on that, but I think it's very exciting project. So, if the proof of concept works, it could be a new line of business.

Then, we're also working on our secure home gateway project. The main reason is today IoT device in the home network with today's technology that we have in home networks, they're most likely enabled to do damage on the Internet. So, all the light bulbs, smart fridge, smart toaster, all of that stuff – all the actuators and sensors – inside your home are allowed to connect anywhere on the Internet and they're allowed to send all the bad traffic on the Internet and participate in DDoS and all the malicious stuff that goes with it.

So, we're building a home gateway that has a new framework inside to make sure that the IoT inside the home don't cause any damage on the Internet and also protect IoT in the home from Internet attacks. So, it goes both way.

So, we're collaborating with DotIT. We're collaborating with DotNL. We're working with [NIST] and a bunch of other organizations on trying to make this a framework.

So, the main reason we're working on this is we don't want a [inaudible] attack to attack DotCA. So, that's one area that nobody is focusing on, so we're taking that piece on to try to make it better Internet.

Then, at the same time, while we're working in the home gateway, the other thing that we notice is today in order for you to reach an IoT device inside your home, it means that your IoT device, like your camera, has to stream, send the data in the cloud server somewhere and then you on your mobile or whatever, you need to connect to the cloud service to view your data. You don't know where the cloud service is and you don't know who's looking at your data and there's a lot of privacy issues around that. It could go to any country in the world. And it's up to the maker of the IoT device to decide where the cloud service is.

So, what we're proposing as part of our project is for every home gateway to have a domain name, preferably DotCA, and then that way you can do a VPN connection to a domain name which is your home gateway. And instead of streaming the camera to a cloud somewhere on the interweb, you stream it directly to your phone. So, a domain name per home gateway is kind of important, in my view. And that would make the Internet safer also, or people safer.

So, that's the two main initiatives we're working on. The security IoT registry, there's more information around it. We're going to show more details as time goes. I think it's pretty cool. We'll have time for questions at the end.

KATRINA SATAKI: It's the end.

JACQUES LATOUR: This is it? This is not the end? It's the beginning.

CRISTIAN HESSELMAN: I also included a few examples, two example projects that we're running at SIDN Labs on IoT and IoT security. The first one is a project called SPIN which is an acronym for Security and Privacy in In-Home Networks. It's actually the building block – one of the building blocks that the secure home gateway uses, CIRA's project. Its purpose is to also prevent DDoS attacks from IoT devices on infrastructure operators such as DNS operators. Basically, what it does is, at least the current version, is monitoring the network traffic in people's home networks, doing that locally so it doesn't share any of the measurements outside the home network with cloud providers, for example.

And based on average statistics, it tries to detect anomalies in the network traffic. When that happens, it blocks that particular IoT device on the network. So, it's a fine-grain blocking. That's what we call it. Which is different from how ISPs currently block your Internet connection if you're infected with a botnet, for example, because in that case they simply disconnect you altogether. So, your entire connection will be gone, including the Internet connection for all of the devices that you have sitting in your home network. So, that's the SPIN project.

Then, also, part of the SPIN project is a traffic monitor. So, this is more about the transparency of the Internet of Things which I think is also a major challenge going forward because people see their IoT devices, if they see them at all, and they interact with them in a passive way, as we talked about at the beginning of the presentation. But they have no idea what these devices are actually collecting about them and with whom they're sharing and under which jurisdiction these data sets are being processed.

So, this is something that we're trying to unveil using the DNS traffic monitor for IoT users, so that's what you're seeing on this screenshot. This is actually something that runs in real-time. If you turn it on, you see all these blobs moving around as new devices come on board and as, let's say, the devices – so, the gray blobs in the graph are the devices and the blue and green ones are the services that they connect to on the Internet. And you see them appearing as they make connections, as the devices connect to the remote services.

The second initiative I would like to share with you all is what we call a national DDoS clearinghouse which is something that we're setting up in the Netherlands but also trying to deploy that on a European level, which is about a system that collects characteristic of DDoS attacks and shares them with other infrastructure operators.

So, there's an example in this graph that shows provider [inaudible] in the middle of receiving a DDoS attack from a set of DDoS sources and it creates what we call a DDoS fingerprint which is a description of what the DDoS attack looks like in terms of what traffic does it convey, what kinds of protocols are involved, what IP addresses and all that sort of stuff. It sends this information to a clearinghouse and the clearinghouse sends it to other service providers and they can then reconfigure their networks, so that they are prepared for the attack in case it comes their way later on. So, service provider two is still out of luck because they need to handle the DDoS attack, but the other ones are becoming more proactive.

So, this is I think an example of what is generally referred to as collaborative security. We're currently setting up a pilot with ten partners in the Netherlands. This includes government agencies but also banks and large ISPs and we're also involved in a European project called Concordia, in which we're trying to scale this concept to European level.

So, in conclusion, we think that the IoT rule is going to bring us lots of new services and we'll actually have the potential to make a more sustainable and smarter society. But there is also a bunch of challenges that we need to address and they are about seizing these opportunities that we identified in SSAC 105 an also to, let's say, mitigate the risks that we identified there.

We also believe that there is opportunities for ccTLDs to play a role in this space. So, one of them would be as an IoT trust anchor, such as what CIRA is doing for their secure IoT registry. ccTLDs could be initiators of collaborative security efforts such as the [DNS] clearinghouse we talked about. And they could be initiators of security mechanisms that are currently not on the k yet and they could try to stimulate the development and deployment of these systems, for instance, by developing the software and making it available as open source.

Also, I think there is ample opportunity to carry out research on IoT security, for instance, using IoT honey pots which will give you more insight into – which will give the community, ultimately more insight into the evolution of the IoT and how it makes use of the DNS, for example.

And we could leverage the mature DNS infrastructure more and better to actually help the IoT through help protecting the physical interaction between the IoT and the physical world.

That concludes our presentations. We blocked ten minutes for questions, so we're right on time.

KATRINA SATAKI: Thank you very much. So, are there any – I see.

BRETT CARR: Thank you very much. That was a really good presentation from both of you. Brett from Nominet. I really liked the home gateway thing. It's really interesting. But I wondered if you had come up against any problems with the broadband ISPs in Canada for deploying it? I think if we tried to do something like that in the UK, BT would go berserk.

JACQUES LATOUR: So, what we're trying to do is we're not trying to build a secure home gateway. We're trying to have the framework to have a secure home gateway inside [inaudible], to start. So that when somebody builds a home gateway in the future, a couple of years, they download the package. It's got a framework in place to prevent IoT attacks and then everybody uses it.

BRETT CARR: So, it's not to replace the incumbent ISPs gateway, then,

JACQUES LATOUR: No, it's for make sure that everybody … Because they all use open [inaudible] or a different version of. So, we want that framework to be imbedded. You want security by designing an open source there. So, [inaudible].

UNIDENTIFIED MALE: I think the point that Brett raises is a very important one because if you really want deployment, there are two ways to do it. One is that everyone puts a dedicated device in their network at home which is something that probably won't scale. The other approach would be to be able to get the software, be the secure home gateway or spam or whatever into the home router of people. And that requires collaborations with ISPs. And then you have to—

UNIDENTIFIED MALE: You've got to engage with the ISPs.

UNIDENTIFIED MALE: Yeah, but they also need to have control over their manufacturers because they need to tell them, "Okay, we need this functionality on our systems."

JACQUES LATOUR: Yeah. It's got to be a collaborative effort.

UNIDENTIFIED MALE: Yes, absolutely.

UNIDENTIFIED FEMALE: My name is [inaudible] from DotIT registry. As an example as a registry that is working on IoT security, we asked staff to collaborate with CIRA and SIDN on how to [afford] home gateway. How it works [inaudible] standard that is the manufacturer use [inaudible] that is – how to describe it? Like a document associated to an IoT developed by the manufacturers as the words say, that tries to describe the usage of the IoT of the device.

The problem of this [inaudible] as it is developed by the manufacturers that it does not take into account the local behavior of the network. So, we tried to introduce some attribute that describe the more efficiently the behavior of the local behavior, like for example the time in which the IoT is used, the range of time. Or, for example, the encryption of the communication or other stuff, the technical stuff, that now is not the place to explain.

And other things is [inaudible] is not developed to described a smarter device. For example, smartphone or iPad. They describe the behavior of stupid device or simple device. So, [inaudible] for example iPad which communication changes on the basis, for example, the app that you used.

UNIDENTIFIED MALE: Thank you.

KATRINA SATAKI: Lise, please state your name.

LISE FUHR: Well, there was no question in the other? Well, I'm Lise Fuhr. I represent the European telcos, the Trade Association in Brussels [inaudible]. Thank you for some very interesting presentations and coming from the telco side, I'm of course very interested in how we can accommodate some of the work that you're actually trying to present and work out on the DDoS attack and the IoT in general.

So, I have one political statement and I have a more technical question. One is, of course, we as telcos are very eager to work with you on this. I think this is essential that we work together on it. I also believe that, if we don't, we will actually lose the trust of the consumers.

And I know that this community is very well-known for working with security but we see in Brussels security is high on the agenda, so I know the telcos are ready to work with you on this and I think we should try and reach out to the different groups there.

So, to Brett's point, I think if we work together, you will not have anyone going bananas on this.

The last thing is, it's extremely interesting to see how you can detect DDoS attack and I'm also curious to see how do you see AI change the way you can detect and actually prevent many of these attacks?

CRISTIAN HESSELMAN: In the SPIN system, we currently have a hard-coded anomaly detection algorithm. So, that's something that looks at the number of connections that are being made, averages it out over time and then when there's a deviation, it raises it more. But you could make that much more intelligent by, let's say, looking at the data for a lot of periods of time, see what the devices are doing. So, basically, calculate their normal behavior and spot any deviations from that. And that's something that we're currently looking into.

KATRINA SATAKI: Thank you, Danny, please.

DANNY: Danny [inaudible], registry in Sweden, but not that well-known to the CEO for the Canadian railway company. Very interested in IoT registry. How would you pitch it for the Canadian railway company that would have a lot of [senses]?

JACQUES LATOUR: I do have a pitch for that. So, to answer that, one way would be between the IoT device, which is mobile IoT 5G and the mobile operator. So, that's where the infrastructure for all the telco mobile operator would be, so the bottom line.

What this framework does is, in the registry, when you take the credential that needs to go in the IoT device, we encrypt that with the public key of the SIM card. So, every SIM card is an HSM. It's got a public, a private key. So, what we do is we use an HSM. We encrypt all the … We create a certificate. We encrypt them in the red box, which is [inaudible] on the registry. That is shipped over the mobile operator encrypted and the only thing that can decrypt it is the SIM card. So, all the mobile operator, depending on the network, they have no ability to do [inaudible] attack. All the content is encrypted. So, that's …

DANNY: We will work together with the SIM card provider.

JACQUES LATOUR: We are working with [GND] and multiple … That's [GSM8]. That's why we're going to join them. Joining them right now. It's to work with the [inaudible], the [G Plus D]. This is totally new ecosystem for us, like SIM card manufacturer. But the new [ESIMS], they're the embedded SIMs that you can put on the IoT device. So, instead of having the SIM card you plug in, it's a SIM card that's embedded on the chip and the mobile operator has the ability to write their profile on the SIM card and we're leveraging that to send encrypted credentials. So, [inaudible] would not be able to intercept any of the traffic, decrypt, or tamper with. It will be encrypted from the registry directly to the IoT device.

DANNY: Thank you.

JACQUES LATOUR: Thank you.

KATRINA SATAKI: Thank you very much. I think that was a very interesting presentation. Certainly something to think about how we're going to shape the Internet, how we're going to provide the service and ensure that domain names are being used.

Thank you very much to Cristian and Jacques. With that, we are breaking for coffee. In 15 minutes, we're coming back here.

CRISTIAN HESSELMAN: Bart just reminded me that one thing I would like to ask, if people are interested in any follow-up discussions on this topic, is there any interest for that? A few hands. All right. There's quite a few. Great. Thanks.

KATRINA SATAKI: Thank you very much. There's one more remark from Jacques.

JACQUES LATOUR: Yes. So, after lunch, we're doing a debrief of the TLD Ops BRBCP workshop that we did right after lunch. So, it's like 12:30 we start. So, if you're here at 12:30, you're going to hear the story. I think it's a pretty good workshop we had and we should all hear about it. So, be there on time. Regis and I don't want to be alone in the room presenting.

KATRINA SATAKI: Well, you won't and we will move some chairs from the table here to the back so that there are enough chairs for everyone who wants to listen to the next session that's on ATRT. It will be chaired by our member on the Accountability and Transparency Review Team, Demi. So, be here on time.

By the way, when you're leaving for coffee, leave through those doors because there's Byron giving away traditional Canadian food. Oh, there's Alan, too. You can use these doors as well.

JACQUES LATOUR: We'll try to start the new session. Please take your seats as soon as you can. Thank you.

BERNIE TURCOTTE: Ladies and gentlemen, we are ready to begin, if you would be kind enough to take your seats. Thank you.

DEMI GETSCHKO: Okay. Thank you, Bernie, for the help. Very appreciated. We are here to take the next session is about Accountability and Transparency Review. We have here on the table Cheryl Langdon-Orr and probably Pat Kane will join us in a very brief time. And also Bernie Turcotte.

Just to say very briefly this is the third ATRT review. The first one was 2010. Each five years we have to do one of these reviews. The second one was 2014. And just to take some notes, there was 13 members in that group. There was two from At-Large, two from GNSO, two from ccNSO, three from GAC, one from SSAC, two independent reviews, and one from ASO.

The third ATRT began this year and have a sharp time to have to finish it in one year. We have 18 members. The eight members came from: At-Large, four members; GNSO, seven members; ccNSO, one; SSAC, three; there is one representative of Board, Maarten. One from GAC. And it comprises 18 members, as I said. I remember the bylaws stated that it has to be until 21 members. We don't reach 21. We fall short of this and keep 18.

Then, we have at the table, as I said, Cheryl is from At-Large. A long-term participant of ICANN. We have illustrious members here at this table. I will pass to her to explain us more or less what we are doing with ATRT-3. I am one of the members but I missed the last two face-to-face meetings. I am in a very bad position here to tell something about the work of the group. But I am totally confident that we will have a very good image from representation of Cheryl. Please, Cheryl.

CHERYL LANGDON-ORR: Thank you very much, Demi, and do not underestimate your contributions at all. Missing a couple of the face-to-face meetings in no way has limited your contributions. You've been a [inaudible] during our weekly meetings. Yes, we do meet a lot, people. So, weekly meetings. And there's no escape from them. There is also weekly meetings topped up by the work party meetings and we did discuss our structure and function last time we met, so we won't be going down that pathway again, but Demi is a vital piece of our team work and I want to thank you all for sending us such talent.

There's a few other members of our review team sprinkled around the room. I may miss one or two but I certainly see Jaap. I see Vanda. I see Sebastien. I see Wolfgang. And I see Daniel at back. Yes, you've got a good sprinkling of members here to visit you today. And of course we have our fabulous staff and Bernie who is a consultant but one that we couldn't do without. He actually takes all our gibberish and puts it into some semblance of the English language, which is no mean feat, I can assure. Let's have the next slide. And we'll be skipping through a couple slides. Pat should be joining us soon, but if he doesn't, so be it.

What we're going to take you through today is a bit of a whirlwind tour on what ATRTs are, but I think, in fact, Demi has done a more than adequate job of that and the background of us, and again I think Demi has done a more than adequate job of that as well so we're probably going to jump pretty quickly to looking at the sources of information that we have looked at and the topics that we are going to be assessing as we come towards our reporting period.

Particularly, we'll take a few moments to look at the ATRT-2 recommendations and the implementation reports associated with the ATRT-2 recommendations, our own ATRT-3 survey. I want to thank you all as an entity as well as some individuals who filled in that survey. Those data points have been invaluable to us in our analysis.

Accountability indicators. Gee, I wonder if I asked how many of you have looked at the published ICANN accountability indicators lately, what the result would be. Won't embarrass you all by doing so but think about it. When did you last look at them? They're published. Are they effective? If you don't look at them, it's hard to know. But yes, we are digging into that as well.

The important issues of prioritization, moving onto the next slide. The important issues of reviews. The diversity on the Board is something that we've been told, as you will see, from the community is an issue for us to grapple with. We've also been asked to look at the matter of public consultations and what constitutes a public comment versus a reaction to a blog or some other thing. And the policy development process (PDPs).

With that, we'll give you a little highlight on where we think we're going to and when after that. And of course we will take questions at any time. So, if you've got a burning issue, just step up to the microphone in the way you are all used to doing so, and we will do it as we go through. Thanks, Bernie, and again moving on.

So, this review team is under different operating guidelines than any other review team before it. We have now accepted a whole new set of operating standards for specific reviews. They were introduced actually after we started, although we did operate under the draft guidelines, so we're not going in one direction and jumping back to another.

But what happened with this is it's going to necessarily alter and limit the way review teams function and make recommendations in the future. Certainly going to make a difference to how we are going to be making recommendations or otherwise, as you'll see a little bit later. But it certainly has given a very defined framework for us to work in, and in particular a number of gating questions we need to ask ourselves when we are contemplating making a recommendation. Let's move on. Thanks, Bernie.

Some of the things, just the highlights, the holidays, about the new requirements for making something a recommendation. We have to [inaudible] identification of the recommendation, the desired outcomes, including metrics used to measure and whatever the goals are that need to be achieved. Need to be clearly stated. We have to have a problem statement that's associated with it. There has to be a ratification of that problem statement by specific data or developing a metric that goes with it. There has to be a suggested timeframe associated with a recommendation, which is indicating what type of measures in terms of its success and efficiency needs to be put into place as well.

We also need to look at whether or not there is data retention of anything relating to our recommendation by ICANN, if there's any industry metrics to support the recommendation. We have to specifically outline what the community input is or whatever surveys or studies have occurred in the development of our recommendation and we of course need to say what degree of consensus there is on the recommendation. And at this point, I feel like going [deep breath] because that's a long way off. We think it's a good idea that … And previous review teams tended to be "we think it's a good idea that you …" Let's go on. Thanks, Bernie.

So, one of those that had the luxury of saying, "We think it's a good idea that you …" was the last Accountability and Transparency Review Team. And it did its work wrapped up in December 2013. The recommendations that came out of ATRT-2 and it's our mandate to look at the implementation of the recommendations from the previous Accountability and Transparency Review Team. There were 12 recommendations with some 46 distinct components. The majority of these recommendations were actually focused on the Board and the GAC.

And the end of 2018, I think September or October if memory serves, report published in 2018 indicated that the recommendation implementation begun in 2014 was complete four years later in 2018. And if we can then move on, Bernie. We can skip that because we know all about that. Although I will mention that our 12-month date comes to term on March 30th because we started our work on April Fool's Day which always amuses me. And I like to be amused. But that's all being covered already by Demi, so we can move on.

What we are going to be doing with regard to our reporting, we've made a conscious decision to minimize, and not just because of the gating that we've just gone through … Welcome, Pat, I had offered your apologies. Thank you. That the gating standards that are somewhat new upon us, but also because we want to make the most meaningful impact, the timely and most priority in recommendations. So, you're going to see less recommendations from us. Not just because it's harder to make them but we want them to be meaningful.

But you are also going to see a lot of suggestions, and in some cases, strong suggestions from us on things that ought to be done. And we're also going to hope that this use of suggestions and strong suggestions makes it a precedent for other review teams to come. Thanks, Bernie. Next slide.

Let's have a look at some of what we found out about, and with this, if you've drawn breath, do you want to jump in or do you want me to continue? I'm happy to continue.

PAT KANE: Go ahead.

CHERYL LANGDON-ORR: Okay. I'll hand it back to you in a little while. In the report of October 2018, as we stated earlier, the report said that 100% of ATRT-2 recommendations had been implemented and here are our findings.

Our findings are that 53% of them were in fact completely implemented. That's a new definition of 100%. We'll work on the math later. 29% were partially implemented and 18% were not implemented. We'll hasten to add we were very purist – [inaudible] smiling. We weren't smiling to start with it. We're learning to smile about this now, but to start with, we were not smiling. I can assure you. Nor is this, unfortunately, unusual. There's yet to be a specific review team that has not discovered – not necessarily these exact numbers but numbers that tend to be more disappointing than delightful regarding the reporting of implementation and the actual implementation.

We were very purist and we took, to the best of our knowledge, what was the intent of ATRT-2 and we looked at was what they asked for implemented? Now, in some cases, because this was recommendations made still under the Affirmation of Commitments, it was pre-transition. We realize we have a different ICANN now than we did then and some things probably were recommended that needn't be implemented. But that's not the point. They weren't implemented and that's what we're reporting. And now you should have settled enough to continue on with the next slide.

PAT KANE: So, one of the things we did as part of the process is conduct a survey of structures and individuals within the ICANN community and what we got responded was 15 of the SOs/ACs provided responses and then 88 individuals responded to the survey and 50 of them answered all of the questions that we had in place.

What the strongest recommendations that came back from the community were around prioritization, organizational and specific reviews, diversity within the Board, the public comment process and support for Board decisions.

Given that there was strong support on the Board decisions, we did not include that as part of one of the things we're going to consider as part of ATRT-3. We decided that, based upon some of the responses in the ATRT-2 recommendations that we would include the policy development process, but the list of the priorities that we put in place were prioritizations, specific and organizational reviews, diversity within the Board, PDPs and the public comment process.

One of the areas that we're taking a look at as well – did you cover the accountability indicators ahead of time?

CHERYL LANGDON-ORR: No.

PAT KANE: Okay. So, the accountability indicators, which is some of the metrics that ICANN Org uses to measure themselves, we're taking a look at those. We have just started deliberations on those so we don't have any leading – or recommendations that we're looking at at this time. We're just going to continue t go through that process.

So, prioritization. In the survey, this was overwhelming in terms of structures and individuals responding to say that the ATRT-3 should take a look at prioritization, which is not surprising because it's a topic here with either the multi-stakeholder model evolution that Brian Cute is leading. We sat in a panel yesterday afternoon where some of the board members talked about the paper that they have put together. So, it is a major topic across the community.

We just got that paper. We're taking a look at that. We're assessing that and that will work into how we take a look at our recommendations around prioritization.

The reviews. When it came to the reviews, there's a lot of things we're taking a look at. The very first thing we're taking a look at is the results of the CCTRT recommendations and how the Board responded. So, for the first time, we've seen kind of a line-item approach to how to dispose or how to address each of these recommendations and where the Board accepted seven, there's some that are pending, some were assigned to GNSO from a policy development standpoint. So, that's the first time that we've seen that and so we're considering that in terms of how we are taking a look at ours.

Also, I know that Cheryl touched upon this [inaudible] slide that the recommendations or the standard operating procedures of what the threshold is for having a recommendation.

So, in response around specific reviews, there clearly is dissatisfaction with the specific reviews across the community and across individuals. So, again, there was a mandate really in terms of the percentage of responses that we got back from the survey to take a look at specific reviews, as well as – next slide, please.

Organizational reviews. Again, dissatisfaction with the process. When we take a look at reviews, we're not just looking at the actual review. We're taking a look at the implementation aspect of reviews. We're looking at that as one whole review includes the implementation process as well.

So, when we took a look and said, "What are we trying to solve for within the reviews?" Now, I think that we have achieved consensus within the ATRT-3 that reviews are an issue and the reviews are a problem and clearly the survey results put that back as well.

What we have not achieved consensus within the ATRT-3 is what we should do and how we should address those reviews. So, we're still in deliberation. But what we took a look at and said, "What are we trying to solve for?" one of the things that we're going to discuss as it pertains to what our solutions look like are these items right here. Lack of coordination and overlap between reviews sometimes results in conflicting recommendations. There are too many reviews. The reviews have to compete for ICANN's resources upon implementation. Lack of time and lack of resources for the reviews themselves. Failure to properly implement recommendations and reporting of this. Again, that goes back to the 53% that we saw as completed. And after six years, if we're only getting half of the recommendations done, one of the questions is were there too many recommendations? How did it change? And why isn't anybody yelling? Half of them weren't done.

CHERYL LANGDON-ORR: We can't be all critical.

PAT KANE: I mean, they were meaningful to ATRT-2 but are they still meaningful today. And because we have a siloed approach to organizational reviews and specific substantive reviews, it's difficult for us to get a holistic view of the organization, the community, and how it works together as opposed to just distinct parts.

So, one of the things that we would like to ask and get some feedback today is where do you think that leads to? Some of the things that we're talking about is taking a look at each of these substantive reviews or organizational reviews and either trim them down, put time-binding on them, do something with the existing reviews or roll them into a single substantive review where everything is accountability and transparency. Move RDS, more SSR into a single substantive review and then take a view of the organizational reviews from the perspective of maybe not just look at the organization, look at the white space in between the organizations now they interact together or one wholesome top-to-bottom review itself.

So, we'd like to ask questions of the ccNSO in terms of what are your thoughts around that? What questions do you have of us in terms of what we're thinking in this particular area? So, I'd like to throw it out. Yes, Jordan?

DEMI GETSCHKO: Please, if you want to make questions, come to the microphone, please. Say your name.

PAT KANE: We only have 30 minutes here, Jordan. Come on.

KATRINA SATAKI: Thank you very much. Katrina Sataki, [DotLV]. Personally, I like the last one the most. The question is who would be the body that would carry that one single review? What are your thoughts?

CHERYL LANGDON-ORR: Embryonic. Sorry, my answer was embryonic for the record. And it is exactly that. Whatever the design is, some of us believe it should be designed by the community, so it gets buy-in from all of the component parts of ICANN. So, it might be presumptive of ATRT to do more than say of these preferred options, dear community, maybe you should be looking at the following … And some of it could be implementation. Some people, for example, believe it could and should be totally third party unrelated to ICANN, [KPMG] or something. Others believe it does need to sit firmly within the bosom and warmth of the community. But whatever it ends up to be, it has to be something that the ICANN community buys into or it probably won't succeed. So, back to embryonic. Pat?

PAT KANE: So, we talked about this a little bit within our discussions but it came up yesterday in the review with the Board on their paper is that if you have a continuous improvement process, how does that particularly work from a group that spits out pieces of discrete work to be done on an ongoing cadence to where we've got small pieces being done and not one megalithic review.

KATRINA SATAKI: One more thing. When the ccNSO Council submitted our comments to the question about streamlining reviews, organizational specific reviews. We noted that one of the things that has not been addressed, when those reviews were initially designed, we were a completely different ICANN, just as you said.

Now, we are empowered community. We're decisional participants and one of our arguments was that according to the bylaws independent reviewers, when they review, SOs/ACs one of the questions they had to answer, whether that particular SO/AC has continuous purpose within ICANN.

So, our argument was that independent examiner has no power to say that a decisional participant has no continuous purpose within ICANN structure.

Have you also looked at the bottom of the issue, what those reviews address and how they are going to fulfill the purpose? Thank you.

CHERYL LANGDON-ORR: Well, yes, we have and, yes, we are still doing so. We're formulating our recommendations at this point in time but all your points are issues that we are aware of, not the least of which is the difference between where we were when these original organizational reviews were put out as an accountability measure and where we are now.

And of course we also have recommendations in work stream 2 which are only currently being implemented regarding accountability of the newer model of what ICANN is. But an ATRT is the only vehicle we have to make changes to these review processes.

So, our recommendations on this area is an opportunity for us to deal with these issues and to make sure it fits and is fit for purpose, both currently and with a little bit of future proofing, because right now, you're right. It's not. And we all recognize that.

It's also relatively expensive as an exercise in terms of human time and real cash. And I'm sure that there are other opportunities that might be able to be explored if we do some clever thinking about still making sure we're accountable and transparent and doing the [intent] of continuous improvement.

JORDAN CARTER: Hi, thanks. Jordan Carter, DotNZ. Just echoing a comment I made yesterday on the public session on this, that whole idea of a wall of continuous review all the time seems discouraging. So, I support either one general review from time to time as a check-in, or if there's a need, the specific and org reviews could be [too].

But I think in terms of human time, it's a problem. And in terms of continuous improvement, a review every five or six years is not continuous.

So, if we see it as an accountability and transparency check in on a regular basis that can take a systemic look at how ICANN is working and isn't just in the silo, then designing that process, you might like to recommend as an ATRT that some kind of a non-siloed cross-community effort be done to design that review system.

I guess the caution I would give is that we can be a very inward-looking community and we may try to design a review process that avoids making hard suggestions and stuff. So, I think we have to hardcode in a degree, an aspect of independent review being part of this. If we sit here and slap ourselves on the back and review ourselves and say everything is fine, then the various powers that be in the Board or community that don't know much about ICANN are going to have legit questions to ask. So, thanks.

CHERYL LANGDON-ORR: Thanks for that, Jordan. As you know, I furiously took notes during your intervention yesterday. That's why I'm not taking notes again today because I think I captured most of it. But that's not unusual thinking if you look at critical control issues and audits and ISO 9000s and 1400s and all those sorts of things which many of you in this room are very familiar with. You have your internal audits with an occasional external check. So, there is no reason that any future model could not include that sort of current best practices design out of the standards world as well.

And do remember that there is always the opportunity to bring in outside expertise. That could be outside expertise in the matter of auditing and designing these things. So, we shall see. Just don't know yet. Nick?

DEMI GETSCHKO: Please, last question.

NICK WENBAN-SMITH: Nick Wenban-Smith, DotUK. Just my observation, being involved in the present review which we have for the organizational review, it's not surprising at all that it costs so much money because it's very thorough and the term "review" is not defined in the bylaws. You just have an independent review. And there must be a lighter way to do it.

But then it also overlaps with work stream 2 stuff, so then what are we supposed to do? Do them together, do them separately. So, there must be quick gains in terms of efficiency.

I'm worried about one massive mega review taking many, many years to do and the frequency of how that would happen. That's my main concern. But there must be some quick-win efficiencies from how that process goes on. Thank you.

I was going to say ATRT, wasn't that a character in Star Wars? Anyway, thank you.

PAT KANE: So, Goran does call us R2D2. So, certainly that was that. If we take a look at – and I know Cheryl mentioned this earlier as far as ATRT and I know everybody knows this is that we've got a one -year mandate and I think that helps keep scope control in place, in terms of you can only look at so many things knowing that you have one year. So, part of the conversation that we're having in terms of the reviews itself is do we time bind it to something that is one year, it becomes broader and we push thing together in maybe 18 months. But that's been helpful in terms of how we take a look at what re the priorities for ATRT-3 and what we intend to address.

DEMI GETSCHKO: Byron, last one. We are short of time. Please.

UNIDENTIFIED MALE: It's his country.

DEMI GETSCHKO: The host.

BYRON HOLLAND: This is a really quick, practical question, not the kind of deep questions we just heard. I'm just wondering, you went through the feedback that you had received, 88 individual submissions, the submissions from the various communities. Do you believe that you've had enough feedback to give you meaningful and substantive input? And how do you feel that that confers legitimacy upon this process? Are you satisfied you got what you need on that front or not?

PAT KANE: So, Byron, thank you for that. So, I think that because we ended up with priorities coming from the survey and some of the commentary that's coming from the survey along with our taking a look at what's happening with the evolution of the multi-stakeholder model and that the Board is having a discussion really around prioritization of reviews that I think, because we've got so much conversation coming from different areas, that yes, I think we're on the right track.

Now, as we get to the lower priorities, maybe not so much. But the things that we are primarily focused on from a priority perspective, I think between the survey results being overwhelming, the commentary that was included, which if you go take a look at the draft that we have on the Wiki right now, you'll see some of that commentary included in the paper.

I would have to say yes for the high priorities. Maybe we could use more on the lower priorities, but I think we're heading in a right direction that's beneficial to the community.

CHERYL LANGDON-ORR: So, we are very thankful for the time you've spent with us today. We really appreciate the feedback. You've got a copy of the slide deck. We are open and available. And with that, we'll give you back your valuable room. And thank you for your time.

DEMI GETSCHKO: Thank you for the panelists, Cheryl, Pat, and Bernie. Thank you very much.

[END OF TRANSCRIPTION]