ICANN68 | Virtual Policy Forum – ccNSO: Members Meeting - ccTLD & Covid19
Wednesday, June 24, 2020 – 08:30 to 11:00 MYT

UNIDENTIFIED FEMALE: Hello and welcome the ccNSO session on DNS in times of COVID-19. Please note that this session is being recorded and follows the ICANN expected standard of behavior. If you would like to ask a question or a comment, please type those in the Q&A pod. We will not be monitoring the chat for questions. As a reminder, in chat, please use the dropdown menu for panelists and attendees.

With that, I will turn the floor over to Alejandra Reynoso, our session moderator.

ALEJANDRA REYNOSO: Thank you. Warm greetings, everyone. My name is Alejandra Reynoso. I work for .gt, the ccTLD for Guatemala. I'm very glad to start this second day of the ccNSO members meeting and to chair this session today.

By the way, I hope you all enjoyed the ccNSO virtual cocktail. It was great to see many familiar faces, meeting people, and have you closer, even if for a moment. Thank you to all who could show up, especially remote participation managers who made it happen. If you couldn't make it this time, don't worry. We will definitely have another one for the next ICANN meeting.

Now back to business. Here is a brief summary of how this session came to be. During ICANN66 in Montreal, there were two sessions on the topic of DNS abuse. There was a plenary session and a presentation by [Yrjo] on its DNS abuse prevention system during the ccTLD news session. After consultation with the [in-room] participants during the ccNSO members meeting, the community expressed the wish to organize a follow-up session on this topic at ICANN67 in Cancun. Since the ccNSO decided not to meet as part of ICANN67, the Meetings Programme Committee requested the decision to be organized at ICANN68 instead but taking into account the effects of the COVID-19 pandemic. And here we are.

Next slide, please. Thank you. This session will be divided into two parts. The first part focuses on the operation part, the impact on ccTLD managers. We will have a TLD Ops business continuity and disaster recovery playbook review, how to run a ccTLD in crisis mode, and the ccNSO Internet Governance Liaison Committee contribution on capacity building. After that, we will have a 15-minute break, and then we will start with Part 2. That focuses on DNS abuse. We will see what is DNS abuse and why is it relevant to ccTLD managers, the COVID-19 issues from an ICANN perspective, and then a panel discussion.

Next slide, please. Here is the first part. We will start right off with TLD Ops with Jacques and Regis. The floor is yours.

JACQUES LATOUR: Thank you. We're going to do a recap of the disaster recovery/business continuity plan that we developed. We'll go to the story, and then I think there's a lessons learned here to be done: we develop a bunch of collateral for disaster or business continuity situation. I think we're in the middle of one. It's a good time for a ccTLD to reflect on the current plans, compare that to what we have, and see if you can improve your posture for the future.

Next slide. Normally, our TLD Ops update are super boring. Right now, especially that we're in the middle of the night and there's not much to do to stay awake, Regis and I will do our best to try to keep you awake. So good luck.

Next slide. With the DR/BCP over the last couple of years—I guess year-and-a-half—we started to put the plan together. So you probably heard about it before: our DR/BCP plan documentation. We built a playbook for disaster recovery and business continuity. This was possible because we actually had people contributing to the work. Dirk led the work, and we actually had a documentation plan that was realistic and actually was usable. So that was a good thing for TLD Ops [to] actually produce something.

Next slide. I think a plan is nice. You need to test your plan. If you have a [inaudible] and people don't know what to do, it doesn't work. So what we decided to do in Montreal—many of you were there, probably—is we tested the documentation against a scenario. The scenario that we picked back then was a registry getting compromised. We could have took pandemic scenario. That would

have been more useful, I think, but we didn't know back then. But in there we actually tested the documentation and the playbook and we found a couple of gaps and we made a couple of fixes. I think overall it's very useful to have this kind of document available for ccTLDs, but it's a lot of work for us, for the volunteers, to put all of this together. What we need to do also is keep it up to date. We're not done because we need to update the documentation and the plan.

Next slide. During—well, that's the slide from [another] meeting. When we did the tabletop simulation, we used cards to try to make it easier for ccTLDs, for staff, to understand what you need to think about in business continuity for the planning.

Next slide.

REGIS MASSE: Just one thing, if I can add something. The most important in this tabletop exercise is—there is two parts. One part was the playbook and one part where the ccTLDs tried to see how to customize the idea of DR/BCP on their own ccTLDs. I don't know if it was a premise to COVID, but it was something to think about to see how they can make this playbook useful for them. While it was a good exercise to just not having a general playbook, it was something special for each ccTLD.

JACQUES LATOUR: It's a lot of work to build the DR/BCP plans. In trying to simplify it, you can't simplify it too much that it's a one-pager. At the other extreme, if you end up having too much collateral that it's unusable, then both

extremes don't work. There's a middle ground where it's usable and functional. That's a challenge based on the type of infrastructure, the type of people you have, the type of services you need to maintain. You need to spend enough time to build this to be useable for yourself. What works for [Serod] doesn't necessarily work for AFNIC, for example. So everybody has their own uniqueness for this plan.

On the ICANN website for TLD Ops, all the documentation is available there. It's translated in six languages. So that's it.

Next slide. This is an example of the tabletop simulation. I think registries should take a step back, look at their existing DR/BCP plan to look at how it was activated, and compare that with the TLD Ops documentation to see if both plans—your plans that you have, what TLD Ops—and see if you can finetune your process if there's improvement that can be done. If there's improvement, then we can add it in our documentation. But doing a tabletop simulation is the only way to see if your documentation works/if your plan works.

We have a sample. You can skip two slides there. Here you can see you have an example of how to do a tabletop simulation. Then you can pick your own scenario.

What we were planning to do or the thinking [in the wings] is the Hamburg ICANN meeting to do a virtual TLD Ops workshop. We're not of the details of what we want to do—maybe try to do a pandemic again and then work out the details so that people have that. We give the best practice [to] everybody from this disaster, this pandemic, and then update our documentation to be more usable. I don't know if

that would be useful. Of, if we can predict what the next disaster is going to be, then we can create the documentation ahead of time.

Next slide. Next slide. Yeah. Another one. Next slide. So I guess that's it for TLD Ops. So we did some documentation. We have a playbook. We did some tabletop situation. Now we're living a disaster. From what we heard, the playbook was useful for a couple of ccTLDs to help them with this situation. Then we want to hear about that.

Regis, anything to add?

REGIS MASSE: Yeah. In addition, Kim said on the chat the link [inaudible] playbook. In addition to this document, you've got old material to play the scenario and to play the game if you wan to play it. I know that, since three months, we are playing in a real case, this kind of DR/BCP scenarios, but the idea is to play and to practice these kind of thing to be ready as much a possible when it happens. So you have old material there to try. As Jacques said, we will try to make a virtual situation in Hamburg at the end of the year to practice and to [inaudible] practices in a virtual mode. It will be a new change for us.

JACQUES LATOUR: Thanks, Regis. So that's it from us. That's our update.

REGIS MASSE: Just one thing. We have sent a survey to the ccTLDs to try to have the information of how many ccTLDs have used this playbook during the

COVID pandemic. We don't have the research yet. That we will share with you when we have these results.

JACQUES LATOUR: Would you off-hand know what the high-level results of the survey would be?

Or we can do that later if we have to.

UNIDENTIFIED FEMALE: Sorry about that. I had to bring it up. We did have two people out of eight responses say they uses it as their primary plan, and six people said they partially used it as a reference.

JACQUES LATOUR: That's good. Mission accomplished. Check!

ALEJANDRO REYNOSO: Thank you very much. Can we go to the next slide, please? Thank you, Jacques and Regis, for the summary.

Now we will have a couple of testimonials on the use of this playbook. I'll start. Next, slide. By the way, I was one of the respondents on "that was our primary source for our business continuity plan."

So this is what happened with us. On Friday, the 6th of March, Guatemala declares a state of calamity. We were wondering why since we didn't have any COVID-19 cases yet. So we thought, "Okay. Maybe

the government is overreacting, but we should think about that." So on Wednesday, we thought, "Hmm. Why don't we use this playbook and do a one-page business continuity plan." So we did. To our surprise, on Friday the first COVID-19 case was confirmed. On Monday, we were told to stay at home. So it was over the weekend that we had to put our plan into action. Fortunately, even though we had very little time to exercise it, it was super useful. We managed to execute it as well as we hoped for. There were only two or three things that we missed out, but without it, it would have been a little more chaotic. Since Tuesday, the 17th of March, all operations are being done remotely. We were a little struck by the velocity of this decision, but we kept a little calm since we had a plan and we could follow it and know what to do exactly.

In the following days since the activities changed dramatically, some documentation has been built on top of that because we had only the one-page business continuity plan. But now there's a business continuity plan that is growing, considering all potential risks that we have. So far, that document is building to 76 pages. We hope it doesn't get too tangled up in documentation so we can use it. We did a risk assessment and management of 18 risks. We have 11 business continuity plans that are most likely to happen and for protocols to know what to do exactly.

Also, it was very important for us to take into consideration that we didn't have a document on all procedures on how things are done in the registry. It is available. So everyone knows what they do, but not everybody else knows what everyone does and how they do it. So

there is now this document existing, and it's 51 pages so far that details how do each and every process that we do at the registry. So it was super helpful for us.

Thank you, TLD Ops, for this playbook. It was super useful.

Now we will hear from Barbara. Next slide, please.

BARBARA POVSE: Good morning, everyone. I feel almost like being at the real ICANN face-to-face meeting [inaudible] after such a wild ccNSO party yesterday. So it's good that I'm not singing.

How did we benefit from attending TLD Ops workshop in Montreal? Well, in the Slovenian registry, we are working on ISOC 27001 since 2016, so we have all our information security policies based on this standard. I registered for the workshop of TLD Ops at Montreal, but unfortunately, I had another meeting, so I asked my colleague—she's a lawyer—and she said, "What the hell? Where are you sending me? I won't understand a word. There will be only techies and I will be just looking around and knowing nothing of what they're talking about." But actually she came back from this workshop quite excited and she managed to get even a pack of cards that were rare at the time. She organized the whole team of the registry. We are ten people [since] December 2019.

We had a registry team building exercise and we used TLD Ops' playbook and played this game for the whole morning [on] where we still have some holes and where do we need to improve. Then,

actually, as you all know, it started with COVID-19. Before it really started, especially in Slovenia, we said, "Well, maybe it's time to look at this playbook again." We prepared our first business continuity plan for the case of an epidemic. On Friday, the 13th, Slovenia declared a state of calamity. Of course, we stayed at home. All operations from the registry are being done remotely.

Well, it was obviously very good to play the TLD Ops game, to be prepared. We have to say there were no major issues. We worked from home and are still mostly working from home and actually still developing different business continuity plans for different possible catastrophes.

So, really, thanks to TLD Ops. It was very useful. Even our lawyer was excited. You can really say this is a success if a lawyer gathered all the registry together and made us do it. Thanks.

ALEJANDRA REYNOSO: Completely agree with you, Barbara. If the lawyer is excited, than this is a success. Great job.

We have a couple of hands. First is Stephen, please.

I believe you have access to your mic, now.

STEPHEN DEERHAKE: I do. I don't know how I got a hand up. That was unintentional.

ALEJANDRA REYNOSO: Oh. Well, nice to hear you anyway.

STEPHEN DEERHAKE: Likewise. Cheers.

ALEJANDRA REYNOSO: Bye. We have another hand. David Olive?

DAVID OLIVE: I just wanted to congratulate the group here for putting on a very good presentation so far, and Alejandra, for you moderating it. I just wanted to say thanks and I'm listening and learning.

ALEJANDRA REYNOSO: Thank you very much, David. Can we go to the next slide? This was the review of the TLD Ops business continuity and disaster recovery playbook. Now we will swiftly continue with Patricio Poblete on running the ccTLD in crisis mode. Patricio, the floor is yours.

PATRICIO POBLETE: Thank you. Thank you for this opportunity to share our experience. Also, thank you very much for scheduling this at a time I can be fully awake. This was a presentation I intended to give in Cancun. Then, because of the crisis we have been living through, of course Cancun didn't happen and another crisis quickly showed up. So I merged two things, and this is what I have.

Can I have the next slide, please? Okay, thank you. Well, this is started Chile in October 2019—the 18th of October, which by now has become an important date in Chile's history. On that date, a number of protests began that started growing in size and became a huge movement demanding political reforms and measures against social inequality. We lived through that for many, many weeks. At the beginning, we couldn't imagine that, ten weeks later, this movement was going to be going as strong as it was in the beginning.

Next, please. The next slide, please. During that time, there were huge, massive demonstrations—previous, please. Not the first. [inaudible] fast but not that fast. The previous one. Can we go to the previous one? Thank you. You can see there a river of people, a sea of people, in the Alameda, which is Santiago's main street. Actually, it was simply more than a million people. So you can see how massive this was.

Next slide. These were mostly peaceful demonstrations, peaceful marches, but, as you'll see in the next slide, there were also violent protests. Usually, these marches ended in violent confrontations between the people in that protest and the police, but also there was a lot of arson and looting, both in downtown Santiago and in the outskirts of the city. This was week after week after week.

Next, please. These protests were met with usually, very often, violent police action and there were a lot of police abuses and many violations of human rights during those weeks. Many people actually lost eyes to rubber bullets, and a couple of people even lost both eyes because of these rubber bullets that police were firing, together with

tear gas. By the way, rubber bullets turn out to be not only rubber. They were analyzed in a lab in, actually, my school. They turned out to be mostly lead and silicon with a rubber coating. So that's why they are so dangerous.

Next, please. Now, how did this start? It started with the small raise in the Metro fare in Santiago. Actually, it went from 800 pesos to 830. So it was four cents, US.

If you go to the next slide, you'll see how people, mostly students, starting revolting against this, protesting in the Metro stations, and destroying some of the equipment there.

Next slide. You'll see that the police also showed up in those demonstrations and there was violent repression.

Can we go to the next slide and then the next? Si. So there was a lot of fights in metro stations. Then, on October 18th, the students called for a massive evasion and jumped the turnstiles. Many of those turnstiles were vandalized, and things were quickly downhill from there.

You see, on the next slide, that many students started sitting in the edges of the rails. Essentially, they forced the trains to stop. You just cannot run the trains at all if even in one station people are sitting with their legs dangling there, as you see.

What happened next—next slide—is, in the mid-afternoon, all Metro service was suspended.

Next, please. If you stop the Metro in the middle of the afternoon in a city with millions of people, you'll actually leave millions of people stranded. Most of those people were angry at that situation and confused. As time went on during that evening, a lot of Metro station were destroyed by fires—dozens of Metro stations and trains destroyed in one night.

Next, please. Next slide. I was, in the evening, at home. It took me a while to actually get home because it wasn't easy to navigate—the previous one, please—the streets. But, as I arrived home, I learned that a large building was on fire. That was building was two blocks away from the headquarters from NIC Chile. Of course, that made us all very nervous of what was happening in downtown Santiago.

Now, the next slide. As the weeks went on, those fires kept happening.

Next slide. You can see in the red dots—that's downtown Santiago—buildings that were set on fire and otherwise destroyed.

If you go to the next slide, please, you'll see that the yellow circle shows where NIC Chile offices are located. So we were very close to the epicenter of this movement. All these demonstrations, all these marches, came very close and often were in the same neighborhood as we were. That meant that there were confrontations between protesters and police. Very often, we're caught I the crossfire, so to say. So what happened?

Next, please. And this wasn't just one day. It was week after week after week, as I said.

Next, please. So you'll see that our neighborhood often resembled a battlefield. That was another building burning, again, two blocks from our offices. That was a hotel and a clinic. So what were our priorities at that time? First, keep our people safe. Often it was not safe to go to the office. And also keep our services operating normally as much as possible. Half the country was revolting against the government. Even in the middle of that turmoil, we need to keep our services, as I say, as normal as possible.

So what they would do—next, please. Next slide, please. Well, first of all, about our services, the resolution of domain names was not a problem. We have a sufficient number of DNS servers scattered around the world and in Chile. So it's very unlikely that any of this would be a problem for domain name resolution. So that was one fewer problem to worry about.

Next, please. The next slide, please. We operate a registry and also a registrar. We've been, for a while, in the process of getting more and more registrars. We have actually a large number of registrars now, but, by far, the biggest registrar is still NIC Chile itself. So our registry and registrar services were distributed in several data centers, and some of them outside Santiago. So it was almost not very much of a problem that all those data centers would be compromised or somehow be threatened by all this turmoil.

Next, please. Next slide, please. But, the economy, of course, felt the impact of this. The price of the US dollar in Chile pesos, as you see, went up quite sharply. The stock market went down. So, for a while,

we have a lot of concerns that perhaps the economic life was not going to be as normal as it could have been, that people who have trouble paying for domains, for instance … So we temporarily suspended the active unpaid domains for their renewals. What we do when you don't renew on time is we first suspend the domain and then later we delete it. So we stopped that for a while. A week or two later, we evaluated the situation and decided that measure was not really necessary—people were still able to say—so we went back to the normal situation.

Next, please. Now, how about our people? We decided that most of them should work from home. It was not like now with the pandemic, where the lockdown is an order from the government. Here we were on our own. The order from the government was that you should work normally. You show up for work every day, only that, on many days, you couldn't. So it was just our decision to do that.

By the way, when we did that, we didn't have any legal backing for doing it. We have been playing with the notion of people working from home for a long time, but there was no legislation allowing to do that. But we did it anyway and the times were sufficient for doing it.

But what we found out quickly is we were not ready for everyone to work from home. First of all, we have a helpdesk—people to answer the phone. The phones have to be answered from the office. We were not able yet to answer them from their own homes. Also, we're part of the university, which is a public university, which is part of all the administration of the state. All that works on paper, mostly. So some

paperwork had to be filed every day because it contained financial information, financial reporting, that we were forced by law to keep reporting every day. So some of our administration people had to go. We were not happy with that, but that was the situation at the time.

Next, please. Next slide, please. But public transportation sometimes was very unreliable or unavailable, so, for the people who needed to come to the office, some of them luckily lived close enough that they could arrive in on foot. But, for others, we hired the [inaudible] taxi service. Very often, even for people who came to the office, we had to let them go home early in the day because of what was going on around our building that made it unsafe to stay until very late.

Next, please. Next, please. Some of the staff that needed to file paperwork we relocated temporarily to the university campus. It was ironic because we started in the university campus and we moved downtime because there were often student protests on the campus, student strikes. We didn't go out to be there, but downtown was dangerous and the campus was a very quiet place. So we moved a few of them back there so we could do the work that they needed to do in person.

Next, please. That was more or less the situation until the end of the year. Please, next slide, please. During that time, communication with the user was key. We issued almost daily announcements of changes in the times that they could phone and have someone answer. We reminded them that online services continued to operate normally. And also good internal communication was crucial. We started a

number of different mechanisms so everybody would keep in touch with everybody else because it was a really new experience for us to be working from home.

Next, please. At the end of the year, most businesses shuttered up. You can see how must of them have changed their windows for something more resistant to stones being thrown or things like that or Molotov cocktails.

Next, please. Next, please. Next slide, please. Can you [inaudible]? So we learned some lessons. I'm almost at the end. So when the current crisis changed, we were better prepared. For our helpdesk staff, they could already take calls from anywhere with their laptops. They were not tied up to the office anymore. We have purchased equipment to support work from home for everybody. Not everybody has a piece of equipment provided [inaudible] provided us that they could take home. [Now they have]. Now the university administration has started electronic submissions of almost—not everything but they have kept improving.

Next, please. So this first crisis was like a rehearsal for what was coming. One thing that we learned that was very important is to support our people working from home. We have kept improving their workspaces at home. We recently shipped them better chairs because they think that they have [inaudible] good for working for a month or two but not for as long as we have been working from home now. So they have now professional chairs. We have coffee breakings in the morning and we have active breaks with a physical trainer in the mid-

afternoon. Since working from home is very stressful, especially if you have people who are falling ill, for instance, we're now providing psychological counseling for everyone who needs it. So that's something. As of last week, we have that available for everybody.

If we go to the next slide, which is, I think, my last one, Winston Churchill actually once said, "Let never let a good crisis go to waste." So we think that we learned a lot from the first crisis and that allowed us to be much better prepared for the next one. That's my presentation. Thanks.

ALEJANDRA REYNOSO: Wow. Thank you very much, Patricio. I think we are now all reflected on our own issues and thinking, "Thank God we didn't have so much to deal with as you did." And you did it magnificently.

I would like to take this opportunity to remind everyone that, if you want to ask a question to any of the panelists, please do so using the Q&A pod. We will be replying to your questions over there. So please do not lose this opportunity to ask anything you have on your mind through the Q&A pod.

With that, I will give the floor to Pierre, who will talk about capacity building. Thank you.

PIERRE BONIS: Thank you very much, Alejandra. Thank you all for being here tonight or today or this morning. I'll do a short presentation on behalf of the

IGLC and of the group because it's work that has been done together with the great help of Joke and Bart.

Next slide, please. We have launched a quick survey internally within the group. I'm going to show you some results of this survey but first of all, I would like just to remind us that one of the first tasks of the IGLC was to discuss with ccNSO members that topics that we see relevance for ccTLDs. As you can see, among these topics, capacity building was one of the topics that was of most interest for ccNSO members. That's why we're going to focus on it.

Next slide, please. You see that we have these quick surveys. We have the answers from most of the regions. I'm going to go through the extracts of this survey. Thank you.

Next slide. It will not be very surprising to you of course. Out of the respondents, 80% of the respondents that they were currently performing capacity-building activities. When we say "currently," it's important because we did this survey at the end of March or April, which means that most of the people answering this survey were currently under lockdown and they were still performing capacity-building activities.

Next slide, please. We asked them why they were into capacity-building activities. You can see the range of answers. It's a [inaudible] of what we asked ccTLDs, by the way. It's our missions, not bylaws. After [all, we are network information centers]. It has the capacity-building within the name—Network Information Center. It's expected from our stakeholders. If you promote the usage of domain names,

then you can see a kind of switch from of a goodwill from the Network Information Center to a more commercial approach to develop commercial services and allow the staff and the registries to achieve its goal. That was more about the internal capacity building and to ensure the smooth functioning of then domain name system. Just to point out that a lot of the staff at the registry itself achieved its goals. As I said, it's more. It's very interesting that a lot of people answered that. When we talk about capacity-building, we think of training the people working for the registry, but we focused this survey and this discussion on capacity-building towards external stakeholders during the COVID-19 crisis. We could have done it also for the internal matters, we didn't.

Next slide, please. As I said, to whom is the target? Internal staff was one of the primary answers, and then potential future registrants, governance, registrars, and registries, of course. So this is very obvious. We have all the main stakeholders of the cc's.

Next slide, please. Now we are going to have answers more linked with the COVID-19 crisis. To the question about a potential increase in capacity-building activities, there was a huge [yes]—70% of the ccTLDs answering—that there was even more capacity-building during the lockdown, which was not a surprise for those who are doing more capacity-building of course. But that is something that may be a of interest for all of us and maybe interesting to showcase outside also.

Next slide, please. Now we go to the expectation from the stakeholder during the crisis because, if we noticed an increase of capacity-

building activities during this lockdown and crisis, we could infer that it was not planned as the lockdown was not planned. So most of us did some capacity-building sessions, training sessions, that they know how to do but they were not planning to do at this level of intensity. So it's interesting to look at what was asked our stakeholders and customers: cybersecurity advices, and training, online presence, registering, website building, of course, and also how to fight abuse on the Internet, especially COVID-19 related. At this time of the year, we are not able to tell them that they should register for ICANN68 and follow the very session that we are talking in.

Next slide, please. The impact, concretely, of the lockdown. Of course, en presencia events were cancelled (most of them), but webinars were an enormous success for some of the [inaudible]. I will speak on my personal experience for the members of IGLC. I find other examples, but on the webinars we organized in AFNIC that are dedicated, mostly, to assemblies in building online presence, in one month and a half we touched 17,000 assemblies, which is 1,000 more than the total number that we touched in one year in 2019. So that gives an example of the huge appetite for webinars during this lockdown. Both the guides/publications from ccTLDs were such and [fined] and read. Some of us increased the visits on their websites, especially on the publication part of the websites. Also, the telephone support, if is open to registries and not only to registrars, of course, had to answer more questions about general questions about techniques and sometimes security.

Next slide, please. So any lessons to learn? This is very quick because maybe it's too early to learn lessons because maybe the questions are not behind us, unfortunately. A greater audience online is a huge load for the staff but is easier to attend for the audience. A lot of people said, "By the way, I never attend any of your trainings because it's in the capitol city. It's expensive. I live far." But obviously this is a very good way of touching you.

In terms of [fear] impressions—I think this is something we're going to discuss in the next part of this session—ccTLDs were sometimes seen as neutral and professional and reached out by the media also more, for some of the [members], than usual because, on this technical part, we still have an, I think, image of neutrality that I think is important in this time of pandemic and fear, of course.

So this are good points, by the way. The main question—I'm not going to answer it, of course, now—is, how can we build on that? How can we build on this image of stability, resilience, and neutrality that was so important during the weeks where a lot of people didn't know where to go, where to find the correct information, and were a little bit lost.

With that, I don't remember if there is another slide after. So next slide, please. Surprise. You have the floor. Thank you very much. If there is some questions, I would be very happy to answer it, of course. Once again, a huge thanks to the members of IGLC who have answered and, at the same time, built the survey and answered it, and, of course, to Joke for her great work. If some people think that

it's interesting to share this survey to the broader audience of the ccNSO members, we would be very happy to do so.

ALEJANDRA REYNOSO: Thank you very much, Pierre. So far we have one question on the Q&A. May I ask Kim to read it out loud, please? Or Kathy.

[KIM]: "Good day, all. My name is [Edith Edjou] from the NG ccTLD. Nice presentation by Patricio. It was interesting to know that lessons learned from first crisis were used to tackle/handle challenges during COVID-19. I would like to know if there was specific policies you had to modify, change, update, develop, and get approved as a result of the first crisis."

PATRICIO POBLETE: If you're talking about the registry policies, basically no, although, at the moment that the crisis started, we allowed for one extra month for people to renew their domains. That, again, turned out to be sufficient to solve most problems that people had at the time.

If you're talking about the general environment in which we work, yes, for this current lockdown, as it is actually mandated by the government, there have been emergency measures taken that give a legal basis for us to be working from home and providing the necessary equipment to people and all that. Before, that was really

very irregular. If a piece of equipment belonged to the NIC, it was supposed to be in the office—not anymore during this emergency.

ALEJANDRA REYNOSO: Thank you very much, Patricio. Thank you, [Edith] for your question.

If there is no other questions, let me wrap this part up with some takeaways. The first one is it's never too late to prepare. We never know when we're going to be in a crisis, so why not now? Start preparing to do your first one-page draft business continuity plan. Second, as Patricio told us, never let a good crisis go to waste. You'll never know when the next one is coming. third, also it is never too late to get some training to face disasters.

With that, I will ask for the next slide, please. Remember we will always have the Q&A pod available if you want to ask questions throughout this question to any of the panelists that have been presenting so far. We will break for 15 minutes and we will reconvene at 1:45 UTC. That will be in 15 minutes. So thank you, everyone. Thank you to our panelists for the first part. See you soon.

Thank you very much. Welcome back, everyone. Next slide, please. We will now start our second part of today's session, where we will focus on DNS abuse and the current situation. For this part, Nick Wenban-Smith will be our moderator. Over to you, Nick.

NICK WENBAN-SMITH: Thank you very much, Alejandra. Welcome, everybody, to DNS abuse. It's basically an introduction of the topic and discussion really as to why this is an important topic for the ccTLD community. My name is Nick Wenban-Smith. I'm very privileged to be able to moderate this session and this panel. It is quite in the middle of the night here, so I do apologize if there's confused dogs and things coming into the picture at any point in time. So just be patient with us.

DNS abuse was a topic at the last ICANN meeting, but really it is one of the hot topics going on in the ICANN community. Really, the ccTLDs can't afford ignore and not be part of this conversation, I feel. From my perspective, the national governments are quite interested in legislating in this area. So certainly in the United Kingdom is very interested in what they call harm online. They've had a lot of difficulty trying to define what online harm actually means, but they're pretty sure that it's bad and that somebody else ought to be responsible for removing it from the Internet. In other areas, you'll see—in the gTLDs, obviously—there's a huge amount of conversation about the topic of DNS abuse, so we should have our own little dive-in as a ccTLD community.

Inevitability you start with a few basic statements of principle. Usually people can agree that, when something is illegal in the real world, online is should similarly be illegal. The laws apply everywhere. So there's nothing particularly special about the Internet, which makes it exempt from regulation and legal norms which apply in the offline world.

Where we usually enter this topic is that, in terms of definition of DNS abuse—because lawyers like to define things so that they know what they're talking about—most people in all parts of the community—you'll see here's the Internet and jurisdiction definition of abuse—come up with these five areas of well-known Internet bad behavior. That's phishing, malware, pharming, botnets, and spam. The caveat with spam, after lots of argument, is it's only when it's a vector for topics listed above. Those are the bad things.

So essentially what we can see here is that the technical community can agree that these are bad everywhere and you can get authoritative feeds, which will tell you when these things are happening, which makes it a lot easier for the DNS operators and for the ccTLDs in particular. Quite often, you're dealing with a trusted community of insiders on the technical side. So we're not worried about political interference. We're not trying to judge content. These are usually patterns of behavior you can see within the DNS itself. So you're not going down the slippery slope of being the policemen of the Internet.

If we could move on to the next slide. Thank you. When we start to look outside of the narrow technical abuses, I think most of us as humans would all agree that crime and criminality is happening on the Internet and that we would like to see it reduced. It's just a question of, well, what can we do about it and what's our role in the ecosystem? It gets very complicated because it turns out that, in different parts of the world, something is criminal in one place which isn't criminal in a different place, whereas the Internet essentially has flattened the

world so you're dealing with the same things in lots of different places. So how do you apply different jurisdictional norms across a unified Internet? And then what types of crimes are we really to be concerning ourselves with? If we look at, say, child sexual abuse material in terms of content, it's nothing to do with the domain name itself but it's the content to which the domain name links. It's universal. I don't think there's anything jurisdictional where this would not be illegal content. So it's very difficult as a ccTLD to justify any sort of association with this sort of content. We don't want it. It's not worth it. It's abhorrent and illegal everywhere. I think most ccTLDs have got now processes and policies that they will not link to that type of content. Certainly, in the same way that you've got feeds and notifiers for malware and phishing, you've got organizations such as the Internet Watch Foundation and equivalents in different parts of the world who will essentially provide an authoritative certification of that sort of content.

But now you're looking into the content arena. I don't know if people are aware, but there's a joint framework between some registries and registrars in the gTLD world where they don't just look at, say, the child sexual abuse material but they extend that type of content into online illegal opioids distribution, human trafficking, any specific and credible incitements to violence. So this is now getting into quite a complicated area, much expanded from the narrow technical remit of phishing and malware.

Next slide, please. The lack of universal standards is apparent, particularly at the current time. I think we've all come under lots of

scrutiny in terms of alleged cures and tests for COVID. Yes, of course, incitement to violence I think we can all agree [to] in principle, but how do you decide whether something has been an incitement of violence or crosses some sort of criminal threshold. You're going to have to look at every single piece of content all the time. You get down and there's a spectrum of other types of illegality. Obviously, brand owners and intellectual property have a very strong ear within governments and lobby very hard that intellectual property [crimes] is a very serious offense. Organized crime quite often is associated with IP crime. But then you end up in a more gray area: political dissent and expression of dissatisfaction with your government, whether that's from the political side of things or how they're dealt with in terms of lockdown—too much lowdown, not enough lockdown. These things could all be illegal. How are we supposed to judge what is acceptable and what isn't acceptable? In the UK, for example, there's a very big debate—I know there is in other places as well—around incitement to not get your children vaccinated or that vaccination is some sort of conspiracy propagated by Bill Gates. That causes huge public health issues in these sorts of discussions. So this is all getting into quite an area which is quite outside the competence of most ccTLDs and certainly outside my competence personally. Well, I may have a view but I don't particularly like to monitor the Internet everywhere. There's a very cartoon of some guy—actually, it's probably about this time of the night—whose wife is yelling at him to come to bed and saying, "No, I can't. There's somebody wrong on the Internet somewhere."

Next slide, please. What we're essentially looking at is possibly the role of registries to police content on the Internet—all types of content and all types of forms everywhere in the world. Is that really a comfortable place for us to be? There's a lack of clarity around the boundaries, what our responsibilities are. I've picked this picture here. Actually, this is a policeman who is keeping peace in a gay rights march. So he's actually doing a good job here. He's not trying to remove freedom of expression. He's trying to protect freedom of expression. But that's very much someone's opinion, and opinions differ across the world of our communities. So how do we square those conflicting opinions.

Next slide, please. Specifically I wanted to touch on why this is so important for ccTLDs in particular. It's important for everybody, but what's our particular angle into it? I was reflecting on this and thinking, well, for us, the jurisdictional issues are not so difficult because we normally do have a jurisdiction to which we are tied as a result of being a ccTLD, but we do also uniquely connect to our own communities. It's really important that we perform our role as the registry to match the values of our communities, whatever those are. It's important that we listen and that we try to respond and we reach come up with our own solutions which are right for us and are right for our national communities. Specifically, we do know from many of our conversations that we are all different as ccTLDs, and that's a great thing of diversity and independence of policymaking. We will not be told what to do, and specifically we won't be told what to do by ICANN. But it does mean that we have to have our own credible positions and have reflected on it and to have some of the answers for

some of these difficult questions about, well, why aren't you doing more to prevent crime on the Internet and how can you make the Internet safer?

Just move onto the next slide and then we can go into a more ICANN-specific view on this. I think we all know that we do not have a unique right to be the ccTLD. We're supposed to do this to reflect the values and add value to our national Internet communities. I think increasingly we were expected to have some sort of—I wouldn't say "oversight"—responsibility to act in ways where, where we see harm, we do things and promote policies which prevent or even mitigate it and no more relevant … Especially that everybody is now working much more digitally, the digital revolution has moved forward a decade, probably, in the last three months, and we're under increasing scrutiny to make sure that we are doing absolutely as much as we can, behaving thoughtfully, updating our policies, and basically responding to the environment in which we operate. A

This is my final thought before we move onto the next areas. For the panel in the future to think about, if we don't do this, are we not leading ourselves open to either national legislation, which can directly bite on us because we're all based in our own jurisdictions? So that's perfectly possible. I think, at the moment, politicians are very much in the mood that, if they see something which needs to be done, they will legislate for it. That may be done in haste and it may result in unfortunate unintended consequences, but they will do it. They have the political will and it's a time of crisis. At times of crisis, harking back to the Winston Churchill quote, if it's something that they're quite

interested in doing in terms of legislating, then here's a good crisis. Let's not waste that opportunity. And there's opportunities for intervention on the Internet. Even if there's not direct legislation, there's certainly opportunities to regulate much more closely, regulate content, and put a lot of pressure domestically on the national registry to do more to protect communities. You're looking at increasing inequality. You're looking at, quite often, a poorly educated userbase of the Internet coming online, being susceptible to harm and fraud. These people then complain to their elected politicians, and the elected politicians want to be seen doing something about, even if it doesn't actually make much difference in practice. Ultimately, if a ccTLD isn't doing its job competently in the view of its stakeholders or local government, then there is obviously the opportunity for a more direct intervention. So, if we're not careful in handling this appropriately, it does open the door to existential threats to our own existence.

I think, on that final bombshell, I will move over to the next panelist. Thank you very much.

JOHN CRAIN: Thank you. Good evening, good morning, good afternoon, good middle of the night to many of you. John Crain, Chief SSR Officer at ICANN.

Next slide, please. In many ways, COVID is much like any other event that happens out there in the world. Whenever there's a major event of some type, be that an election, a disaster, political strife, riots, etc.,

there tends to be a surge or a burst in registrations of names related to that. What that basically is is the bad guys moving their focus towards where they think there is a lure or a bait to hook their victims. COVID-19 is really no different than any of those other events from a technical standpoint. What's interesting about COVID-19 is, firstly, obviously it's very global. There's a lot of [extra] related stress on people out there. I think everybody is at some level worried about COVID and their families and their work situations. People are working from home. Everybody is using the Internet. So it's almost a perfect lure or a perfect storm for the bad guys. As ICANN, our focus is mainly on the generic top-level domain space, although there are a couple of country codes that asked us to do some of this similar work and share intelligence with them. So let me talk a little bit about what we did.

Next slide, please. You've all seen large numbers in the press. We've all seen issues where there are hundreds of thousands of names registered that have strings in them related in some way to the COVID epidemic or things associated with that. This is a piece of data from [DomainToes]. I will point you to one word that appears here a couple of times. It's the word "risk." What these are measuring are names that have strings in them related to COVID in some way. What they're saying is there is some risk associated with them. They're not necessarily saying they're bad names or malicious names. They're just saying they're risky names. As you can see here, they peaked out at about 5,000 names a day. It rose and it went down. Our own data at ICANN replicates this.

Next slide, please. And that downward trend, by the way, continues as we go forward. Our approach to actually find the names is to take all the zone files, etc., and look for pandemic-related keywords. These could be very straightforward English-translate[d] COVID, corona, pandemic, mask, etc. They could be things that are just related to them. Chloroquine was a buzzword for a while. They could be translations of those words or local words of interest from other languages, homoglyphs, or slight adaptions of letters or numbers, etc., in those names—stuff that are close. They are also things that we look at, such as white lists, to make sure we have good stuff. But we also looked at things like doing Punycode conversions for things in other character sets. So we looked quite wide and we ended up with a very large list of strings.

Next slide, pleased. This data is actually a couple of weeks old. We've over 7,000 domain names identified since we started looking at them in January of 2020 that have strings that are in some way related to the pandemic or things that are strings that are related to sideways things on that—things like mask and virus—that can also be used for many other things.

Next slide, please. I'm going to try to get through reasonably swiftly because I want to get to the panel discussion because it's going to be more interesting. What's interesting is that, although we looked at hundreds and hundreds of names or strings, as we added strings, we found that a lot of strings don't turn up much. We have strings that only turn up a few names that look like they're suspicious. Some of those may indeed have been malicious, but four keywords actually

took about 73% of the domain names, which is a sign of where the bad guys were focusing. We'll share these slides so you can look at them later.

Next slide, please. But this is data. This is just list of strings. It's not intelligent. There's nothing really sophisticated about this. This is really keyword matching in zone files. Pretty easy to do. We know by looking at this—7,000 domain names so far, roughly—that a lot of these names are actually benign. In fact, the majority of these names may be benign. They may be parked. They may be unrelated. If you search a name or a string like "mask," well, there was a move called "The Mask," and there's lots of other uses for masks. If you look for "virus," obviously there are a lot of things around and antivirus, and there are many more viruses than just COVID. So you actually have to further than that if you're looking for something that is more than just a risk but is actually abusive and malicious.

Next slide, please. The way we do that is we do what we call API calls. We go and look at various systems to whether or not there is information known about that specific name. We've blocked the names out on these.

Next slide, please. One of them that we use is virus total. They actually pull together about 80 or 85 different virus and antivirus engines that look at things.

Next slide, please. [inaudible] is very similar. Once again, it collects names and information around malware. PhishTank is a well known one which is very much focused on phishing.

Next slide, please. And Google Safe Browsing is also a very well respected and very well known repository of data about badness. Now, we focus very specifically, going back to what Nick was talking about, on malware and phishing. Now, much of the phishing data also includes pharming, etc. Many of the lists that we look at don't separate those clearly. The definitions are vague. One person's malware site may be listed as a phish site because the phish took them to malware and one engine decided to list it differently than the other. But we didn't go too deep into that.

Next slide, please. This is the basic reporting data flow. We start with our input. It could be any file, any list of names. It's quite possible that you could come to us as a ccTLD and say, "Look, I found all these names. Could you input into your system and give us a report?" The system will do that if you want us to. Then we filter on these keywords. I call this string-based detection. So we're really just matching strings. If a name within the zone file does not have one of those strings, then we just stop. Then we go and look in all those threat intelligence sources that we were talking about: the APIs, the block lists, and, of course, the allow lists or the white lists. There are names out there that of course include COVID but we absolutely do not want to block them because they are there to help. They are good names. And there are lists out there—what we call white lists or allow lists—that say "Do not block this name." So we include those two. Once we've done that, we look at and we say, "Do we think this is sufficient evidence?" Now, that's actually a manual check. We go in and look at it and say, "Well, who is reporting this? What do we know about the reporter? How

much faith or trust do we put on that particular reporting mechanism?" There's probably, in total, around 100 different reporting engines and bodies within what we look at, but we know a lot about all of them. If there's somebody reporting that we don't know much about because maybe they're not particularly transparent in their process, then, if they were the only people reporting, we'd say, "Well, we don't actually have enough intelligence to say that that's a valid report." If we don't have sufficient evidence, we stop. We drop it to the site. Then we go and look for other kinds of information that might be useful.

The idea here is to gather sufficient evidence and information that we can pass on to somebody who can take action. Now, there are people who can take action in the generic TLD space. It's typically the registrars but it could also, in some cases, be the registry. So we gather the DNS information. We gather some geolocation information. One of the first things we gather is, is it still resolving? You have to remember that we may have taken a zone file an hour or two hours or three hours ago. By the time we go and get ready to report it to somebody, action may have already been taken. A lot of the registries are already taking actions on many of these names. Only if we get to that stage where the name is resolving and we think there is sufficient evidence that somebody can actually take action will we actually forward that to a registrar and say, "Please investigate this." That's what we ask them to do. The ICANN contracts and the obligations of the registries and registrars are to investigate and then take what they deem appropriate action. So we pass it onto them for that purpose.

Next slide, please. If you remember, I said we started with about 700,000 names over this period. That's roughly the 3,000 to 4,000 names a day that we look at, but you tend to lose an order of magnitude at every gating factor. Every step you do in that process actually identifies names that there is no evidence that they are bad. So we remove them. So we get thousands of registrations a day. We get reports on hundreds of them. But, by the time we go and find the ones that still resolve—i.e., nobody has taken any kind of action against them, we don't know what action has been taken, we have no data to support that, and we only know that it no longer resolves—we're actually down to the tens, which is why we can actually go in and look at these by hand because the numbers, when you look at them, of where there's actual evidence of badness—I'm not talking about the level of harm here; I'm talking about the evidence that something had has happened—we're actually looking at fairly strong numbers. If we've gone orders of magnitude down from 7,000, I know we're done to a lot less than 7,000. We're done to less than 700 names that we've reported over the period of time. Even sometimes when we report the name, by the time registrar replies to us, which may be a few ours or even a day later, the action has already been taken because somebody else reported it. So that's what we're doing.

Next slide, please. In conclusion—next slide—there's no doubt that, during something like this—any kind of event … There's bad stuff out there. We all know that bad stuff happens on the Internet. We all know that people register domain names to perpetuate crime and bad behavior. There's no doubt about that. But, if you read the earlier

indicators and a lot of the press—this was what Nick was talking about; governments getting worried and things like this and taking action; this is often what they read—much of that is about names that have risk. They're not about names that are actually being used for abuse. So it's really important that, when we do these kinds of things, we actually go and look further and dig down deeper to find out what's actually happening. I have the privilege of having been able to add a couple more researchers to my team. I should say sorry to Nick that we may have borrowed [Sean] from Nominet, but thank you. He's awesome. But we also have a couple of others. So it's given us the ability to actually apply good science to this and start digging down. We hope to be able to do more of this kind of project where we try and get the data and the intelligence behind what we actually see happening and bring this back to the community, including the ccTLDs, so that we can use it in discussions around how we improve and how we do things better next time.

I think, with that, that was my last slide. Thank you.

NICK WENBAN-SMITH: Thank you very much, John. No hard feelings for [Sean]. I'm glad that he has improved the average quality of the technical staff in ICANN as a result.

JOHN CRAIN: Absolutely he has. If you need to borrow him at some point, [I set beer as currency.]

NICK WENBAN-SMITH: He did a good a good stint at Nominet, so there's no problem here. My goodness. Look at the photos here. You can tell that lockdown has been hard on some of us.

UNIDENTIFIED MALE: I have [inaudible].

NICK WENBAN-SMITH: Anyway, moving on to panel discussion, I think this was a nice segue introduction into this. So we have the DNS abuse topic. We have the COVID-19. It's the perfect-storm intersection of these two hot topics, which is really what we want to explore today. I'm very pleased to be joined on the panel by the four regional organizations/general managers. We have Barrack, Leonid, Peter, and Nacho. I've also still got Regis and Jacques and John, obviously, around. I muted myself for a moment there, classic style. So obviously I welcome any thoughts that they have as well.

My first question is this. There's not any more PowerPoint presentation or anything here because I think we've all had quite a lot of PowerPoint in the last few days. On COVID, John is right in the sense that this is just another national/international crisis and there's always some sort of thing going on. But it is massively significant in terms of global events. In many parts of the world, including ICANN's home jurisdiction, it seems to be some way off to actually getting to the peak of it. Today in the UK actually we've just decided that we're

okay to relax a lot of the restrictions, so that's good. But it's getting worse in many parts of the world. I just wondered, from the regional perspectives, which might be different because obviously everybody is in a different place with the virus, these short-term focuses. As John was describing. We're monitoring registrations with COVID terms. Is that going to become normal? Are the ccTLDs going to have to change the ways in which they operate? Are we supposed to be now monitoring all registrations for "risk"-based terms? Are we supposed to now take a more interventionist view? Is this going to result in actual changes to registration policies that we wouldn't have imagined that we would be talking about only six months ago? I'll ask the panelists in a different order, so they'll have to be alert and on their toes. So I apologize for that. Maybe, Barrack, you can take the first question, if that's okay.

BARRACK OTIENO: Thank you very much, Nick. Good morning, good afternoon, good evening, everyone. This is Barrack Otieno from the Africa Top-Level Domains Organization.

Quickly, from an African region perspective, currently I would say that there is no indication that there would be much change in the registration policies. The effects of the pandemic is getting to be felt right now. We are seeing a marked increase in the number of infections. Most countries are on high alert now. Actually, the region started getting infected sometime in March, which was two or three months down the line after the rest of the regions had been affected.

Having said that, I would like to mention that something unique about the African region is that most registrants do access the Internet through their offices, and the pandemic has resulted in people working from home, which means that a significant number of the populace across the region is not able to access the Internet. Therefore, it has indirectly affected the use of the DNS system. We've seen a slowdown in the number of registrations. Again, for businesses, businesses have not been registering domain names in numbers as such because, again [inaudible] connectivity beyond most of the cities in our region remains a major challenge.

So, just to answer, in the foreseeable future, on the registration policies, we are likely to see a [stethoscope] in the region. We are not going to see any major effect as far as out of the COVID-19 pandemic. Thank you very much.

NICK WENBAN-SMITH: Wow. Thank you. That's a really interesting insight, actually: that it's indirectly affecting access. Thank you.

Next up I think I have Leonid.

LEONID TODOROV: Thank you. Good time of the day, everyone. This is Leonid Todorov of the Asia-Pacific Top-Level Domain Association.

Well, I would agree with Barrack by and large as far as the current situation, but I'm afraid that there is a certain lag between whatever

disaster or calamity and its effect. I would say that, for the Asia-Pacific region, 70% of ccTLD registries are actually public agencies/government agencies. It might have a serious impact, but, as I said, it would be a delayed effect.

Policy makers tend to act decisively, as Nick noted. They would probably take some time to assess whatever potential adverse effects of the global pandemic on malicious registrations are, for example. Then they would tend to legislate. Again, given that these ccTLD registries are mostly government-owned offices, they would have to react.

So I would suggest there should be some change in the way ccTLD registries would treat registrations probably. More policing and more scrutiny to new registrations.

Then yet another thing which we should factor in there is that some of these registries—quite many of them—are fairly small, which means several thousand registrations in the file zone. So that would mean that they would probably be able to cope with these challenges even if they are short-handed.

So I would suggest that there should be some tendency for more policing and more scrutiny. Thank you.

NICK WENBAN-SMITH: Thank you. I hadn't really taken into account that essentially these are mostly government-owned ccTLDs, and a lot of them quite small in the Asia-Pacific region. But that's obviously correct.

I think next up is from the European region: Peter Van Roste. Peter?

PETER VAN ROSTE: Thank you, Nick. Good morning, everyone. Let me first do a +1 on John's figures. I think that's really important to describe the situation that we find ourselves in. In Europe, we saw exactly the same ratios in a large sample across a ccTLD-centered community, even to the level of similar parked-for-sale, low-content domains numbers. So it's interesting to observe that, in some aspects at least, the ccTLDs and gTLDs might have something in common after all.

I agree that these were extraordinary times and they required extraordinary measures. In Europe, we saw two things happening. First of all, roughly 80% of the respondents to a recent CENTR survey indicated that they scanned new registrations for COVID-related terms: COVID, corona, masks, and a few others, like virus, probably. Some ccTLDs started checking the results from that scan for accurate registrant data. If anything was wrong with it, they would have an expedited procedure and allow registrants to correct any inaccuracies. If they failed to do that, then there name would not be activated and not linked to nameservers.

The second thing is that we saw closer collaboration with law enforcement, health authorities, and, very importantly, consumer protection authorities in some of the countries.

I don't think that the manual verification that we saw with some ccTLDs is scalable. Remember, extraordinary times/extraordinary

measures. For some ccTLDs, that took quite an effort. Some went even as far as having to receive written proof of identity from their registrants for those names that were considered to be high-risk. I think we should all keep in mind—well, we do, but inform people that we're having this conversation [but] that we're talking about a few dollars or a few euros product. Manual verification does not work well with that. So there's a couple of caveats here.

However, I do believe that some of these practices will remain, especially those registries that relied on automated tools or even intelligent automated and intelligent tools that learn through the process. These tools could be shared across the ccTLD community. We've all been pretty good at sharing knowledge, as the ccNSO and the regional organizations are a testimony of.

As to your question of whether it have an impact on policies, what we saw in Europe was that a couple of ccTLDs finetuned their policies to allow them quicker response to inaccurate data. Terms typically were something in the order of two weeks' response time to fix a problem. That has been shortened significantly, given the risk and the pressure on this high-profile file.

So, yes, a couple of things are definitely here to stay. Policies will be finetuned to be better prepared for any new global phenomenon that could increase the abuse risks. I think [we'll get] later to that, but there will also be an impact on the way that policymakers are thinking about fighting abuse through all of our industry, for sure. Thanks.

NICK WENBAN-SMITH: Thanks, Peter. Interesting. I see there's a question in the Q&A pod, but before we move to that—thanks, Byron—we'll move on to [inaudible] for the first question to complete the panel.

NACHO AMADOZ: Thank you, Nick. Hi, whatever time of the day you are. Well, I'll be just very brief. I would say we're more near to what's happening in Europe. In some points [inaudible] we're a little different. Just a few of our members have been thinking about changing their registration policies, mostly for registration doing malware, botnets, or phishing. That's DNS abuse. But nothing is decided yet there. At least I had no news from ccTLDs analyzing more checks in times of registration or after that. At the moment, according to a survey we are running—we don't have all the answers—just 19% of our ccTLDs are doing identity checks before registrations, but these checks are not implemented due to COVID. I think we're going to be talking about some other things later, so I'm going to stop here so I don't take more time.

NICK WENBAN-SMITH: Thank you. Jacques or Regis or John, do you have any thoughts on that particular issue around registration policy changes and more checks becoming more universally accepted as normal?

JOHN CRAIN: Yeah. I think that, once you show that you can do something, there is going to be pressure to continue doing it at some level. For ourselves on the global level, we're asking ourselves a lot of hard questions

about how you would identify what is an event and what is not an event. How do rationalize that? How do you systemize this? You can't just say, "Well, it's in the news and therefore it's an event," because most events are regional or national. They're not global like this. Take election events, for example, and election fraud—something like that—where obviously there's pressure. You see the pressure on the platform providers around misinformation—all that kind of stuff. That's not the game we're in. That's purely content. So how do we take what we've learnt and used it in a way that is sustainable and actually pulls out useful intelligence? For us, the goal was to pass on actionable intelligence to people who can do it. If you overwhelm them by getting too loose on this stuff, for want of a better word, that's also not a good outcome.

So we're thinking hard about this. I think the community will. But I think we're all going to much and many thanks from law enforcement and the agencies that we've all worked with that we stepped up. But the question is going to be, how does this continue? So there's going to be pressure. I think it's important that, whatever we do, we make sure it's something that's sustainable and practical in the long run. As Peter pointed out, this is not a high profit margin industry, despite what some people think. So going at $100 worth of evaluation on a $10 or $2 registration is probably not going to work out.

NICK WENBAN-SMITH: I think that's a very interesting point. Obviously, I share totally [the view] that, for the cost of a domain name, there's certain types of

businesses just [un-economic] to accept because the type of hassle that you get in dealing with it in verification and removing it and all the rest of it. It doesn't justify the amount of time.

I've had in my role, I think, six interventions from law enforcement agencies in relation to these types of COVID uses. Actually, of those six, three of them were domain names where the domain name itself did not relate to any of this virus pandemic. They were selling—or allegedly selling—tests for COVID which couldn't exist because they weren't on the market at the time and they certainly weren't authorized for sale by our medical regulators. But it's nothing to do with the domain name. It's one of these interesting dichotomies. You can have domain names themselves, which looked terribly problematic, but the content either doesn't resolve or it resolves to pictures of cats on the Internet. Then you've got perfectly reasonable domain names which have the most horrific content or illegal content. That's always very difficult for the registry operators to do anything about, I think.

JOHN CRAIN: This is why our focus was very much on the type of abuse and not on the content and not on the string. You could add as many words as you wanted to that list related to COVID, but if there was no actual abuse—[or] the risk of abuse—there was really nothing to do.

NICK WENBAN-SMITH: We had a question from Byron, which is around the creation of these lists or sharing lists. His question is, "Were there registries in your regions creating lists or sharing lists with law enforcement agencies that were different or outside normal rules and procedures? And how do you rationalize or justify that sort of list creation?"

I'll take it in a slightly different order. Obviously, we welcome questions from the community, and I think it's a really interesting question, actually, because I'd be surprised if there was any sort of guiding force behind it. We just did what we had to do, but I'd be interested to here.

Leonid, in terms of list, I didn't hear that that was particularly an issue in the Asia-Pacific region, but perhaps you can help here.

LEONID TODOROV: Thanks, Nick. Well, I can only speculate because I have no hard evidence. But I would imagine that quite a number of APTLD members have long practiced these lists just because there are certain policies and I believe their governments are vigilant about that. For example, when it comes to Sharia or Islamic, there are certainly measures taken to monitor the zone for purity. That relates to the content. So such practices are quite widespread in certain parts of the region.

When it comes to, once again, smaller registries, smaller-sized registries, it seems to me that it won't happen any time soon. However, I must admit that politicians and policymakers tend to overreact at times, and there might be some kind of new pandemic

when such a trend would spread across the region. I wouldn't rule this out. Thank you.

NICK WENBAN-SMITH: Thanks, Leonid. Peter?

PETER VAN ROSTE: In Europe, there are quite a few registries that are sharing lists with specific authorities. Belgium, for example, come to mind, and the Danish as well, I believe. Some others share it with law enforcement, whereas in the previous cases it was health authorities and consumer protection authorities.

In addition to that, more and more European ccTLDs are opening up their zone files. So I think we can see that. We can expect that more and more authorities will start using that opportunity to do that type of checks themselves. So they will come up with their own lists rather than wait for a ccTLD to provide them with one.

The reasons for the existence and the practice of sharing lists is, of course, that ccTLDs are not in a position to judge the content, but they are perfectly well-placed to see what's coming on the registration end and flag suspicious registrations. One of CENTR's members, EURid, has quite an advanced system that flag these systems. It has been presented in the ccNSO before [inaudible]. That sort of system actually helps narrow down on the potential abuse cases, rather than provide anyone with a big-ish list. That's it for the rationalizing part of it. ccTLD can't do that. Law enforcement can.

An interesting thing is that sort of cooperation, where lists have been shared or at least discussions on what are risky domains … These discussions started during COVID. They look place faster, probably, than people expected. But in Europe they are quite necessary because we are going to see the implementation of a consumer protection regulation—a European regional instrument—that was approved by European institutions about two years ago. It's now nearing the final stages of the implementation across Europe. This was a pretty good test as to what kind of cooperation works, what can ccTLDs do, and what can't they do. Thanks.

NICK WENBAN-SMITH: It's an interesting point about the zone files being accessible to law enforcement agencies because, in a sense then, the ccTLDs don't need to have their own list. The law enforcement agencies can check for whatever terms they want. Perhaps they could their jobs better because that's what they're supposed to be doing, right? That's always been the case in the gTLDs, I think: they've always had publicly accessible zone files. So it's very surprising that there's so much crimes in gTLDs, and ccTLDs are so good.

Anyway, Nacho, in terms of lists and Byron's question about how did the lists get generated and all that kind of stuff, if you've got any Latin American/Caribbean thoughts.

NACHO AMADOZ: No, none that I am aware of. We did some surveys of our members, and that wasn't mentioned at all. We are doing quite well, I think, in terms of DNS abuse, especially in domains with COVID-related terms. In a recent survey we did, we had no more than 2K domain name registered with those related terms, and less than 0.05% of those had any complaints about misuse. So we're doing really well here.

NICK WENBAN-SMITH: So, to that extent, your experience matches the European and the ICANN experience in terms of that, even though you get quite a few registrations, the number of abusive registrations is vanishingly small and certainly probably not out of line with your general abusive registrations, I guess.

NACHO AMADOZ: Mm-hmm.

NICK WENBAN-SMITH: Barrack, in terms of the lists, I didn't hear that the African ccTLDs were really going down this route of scanning the terms and lists. Is that correct?

BARRACK OTIENO: Thank you very much. For the Africa region, it's not a prevalent issue for now, but going by a number of members, there has been questions or concerns being raised. Most of our country-code top-level domain registries also work very closely with the national computer incident

response centers. So there's been questions from the government agencies on how to handle some of the names that are increasingly being registered for COVID-related causes.

Just to paint a picture, in some cases, you find that governments are setting up national websites that, for instance, can be used to raise funds to support COVID-related initiatives or causes. There's been a case of people mirroring these kinds of domains. For instance, if I may use the example of Kenya, you find covid19.ke and someone else doing covid-19.ke. The public is not able to distinguish between these two names. How this has been dealt with is there's a bit of awareness in some of the countries where this effect has been felt.

Just to reiterate what I said when I started, the region is getting to feel the effects now. We will be at a better place by the end of July to be able to give a real picture of the effect that has been had. We are actually having these conversations on a continental level right now. Within this week, through the end of July, a lot of webinars have been lined up in which the key subject is the effect of COVID-19 on the DNS system or on the Internet system.

So this is a timely conversation, although, compared to the other regions, we are coming in a bit late in terms of feeling the effects of the pandemic. But that is the status of the region as it is.

NICK WENBAN-SMITH: Brilliant. Thank you. It's a sobering thought, isn't it? In the timescale, it's still early days, probably. We're probably going to be having these

panel discussions for the next year or so and there'll be more information and more data around what the effects have been. Thank you. Thank you very much, everybody, for that.

In terms of the challenges which have come through, obviously, as we heard in the operational challenges with offices being shut and everybody working remotely and disaster recovery and the business continuity planning, that was quite an interesting session. But I'm more interested in the non-operational challenges—the political or policy-type challenges which would have arisen as a result of this sort of working. I wondered if the panel could give us a little bit about what are the hot areas are across their region because, in relation to what the impact has been, it seemed very different across all the four regions. I wondered whether the challenges would similarly be different across the four regions.

Peter, I think you get this question first, please.

PETER VAN ROSTE: Thanks, Nick. I would identify two main challenges. The first one was fighting bad data. We spent as an industry a lot of time explaining to politicians, law enforcement, and other competent authorities that the numbers that they saw in the press were incorrect. They were so convinced—

NICK WENBAN-SMITH: Fake news, then.

PETER VAN ROSTE: Yeah. It took away precious resources at the time they should have been focused on something else. The analysis that we did, whether it's ccTLDs individually or at a regional level or the fabulous work at ICANN, showed that could have been directed at something else. So, for me, that was one of the main challenges because it was so closely tied to the reputation of the DNS in general and the ccTLDs specifically.

The second one was the big splits that we saw. So the long stretch between "we want to do the right thing but we want to be careful that this is not going to be used against us"—the whole slippery slope story … The only problem is that, at a time of crisis, nobody cares about the explanation or wants to listen to how extraordinary the things are that you do. You seem to be doing them, so it's possible to do them. Whether that's scalable, whether that's long term, whether that applies to additional issues, those looking into some of the chat discussions, whether they were in the ICANN environment or other places where this exchange took place, they for sure the IP rights holders saying, "Great job, ccTLDs. So happy you're finally doing what we've been asking you to do all along for this good cause. So kudos from our side." Of course, we're going to have to continue those discussions with these different stakeholders and keep on explaining what we do.

So the big challenge there is probably in having the resources, the time, and the patience for eternity for explaining what the industry

does, what its limited role is, and, more importantly, what its limited legal possibilities are to step into this [debate] even if you wanted to.

NICK WENBAN-SMITH: Well, I think that education repeat-and-rinse to all of our domestic stakeholders is nothing new. And that's noting new related to COVID. That's for sure.

Nacho, what are the challenges across Latina America and the Caribbean?

NACHO AMADOZ: [I would say I don't know if we saw some future during that. This might help us.] … Can you hear me?

NICK WENBAN-SMITH: We lost you. You just broke up for a second but I can hear you know. I could hear you now.

NACHO AMADOZ: What I was saying is we see the future during 2018 and during the past year, but we did …

NICK WENBAN-SMITH: I think we lost—oh. You're just a bit patchy there. I'll move on to Barrack because we've only go a short period of time left. So I'll move on to Barrack for challenges.

NACHO AMADOZ: I'll take off my video then.

BARRACK OTIENO: Can I proceed?

NICK WENBAN-SMITH: Yes. Please proceed, Barrack. Thank you.

BARRACK OTIENO: All right. Thank you very much. The other general challenge I think that is prevalent in most of the countries in our region and which I think, again, are affecting the region by and large, especially for ccTLDs or registries that are charging for domain names and related services, is that economically we've seen a reduction in non-essential expenditure. Let me put it that way. If I may give a perspective, I think a significant number of the populace in our region—60-70%--are small and medium enterprises. So the COVID-19 pandemic has compelled people to work from home, which means that a number of jobs in the [informal] sector have been lost. So, when you are basically asking someone to spend $100 in registering a domain name and hosting and building a website, they are forced to consider how they will survive for the next couple of weeks or invest in their domain name. We've seen a significant number of jobs being economically where one would say that the answer would be going online, especially for the small and medium enterprises. But the counterchallenge to that,

again, is the issue of poor or underdeveloped [inaudible] connectivity in most of our areas. That is beyond the capitol cities in most of the countries in our region. So it's an issue that policymakers are grappling with. Those are some of the challenges that we have faced on this side.

NICK WENBAN-SMITH: Thank you very much. I was wondering when somebody was going to mention the economic impact on all of this because that, I think, is going to be felt for, maybe, decades. It's still very, very early stages.

Finally, Leonid, in terms of the challenges in Asia-Pacific.

LEONID TODOROV: Well, the region is too diverse—thanks, Nick—to actually apply the same metrics, but I would say that, for example, politics-wise, the ccTLD registries in the region have, for long, been the epicenter of policymaking in the ICT and the Internet area because, once again, they're just very specific arms of local, let's say, ministries or agencies for telecommunications and the Internet. So I wouldn't forecast any drastic difference in the future.

Meanwhile, we should understand also that, in many jurisdictions across the region, ccTLDs are perhaps the one and only ultimate source of expertise when it comes to Internet-related queries and concerns. So they probably found themselves in a peculiar situation now as they are, at all times, called for advice or comments or proposals and recommendations as to how to sustain, for example,

the Internet and the ICT industry in the country and how to ensure a sufficient degree of security. So probably being in the limelight is a good position, but not all the ccTLDs are ready for that. That relates to capacity-building in [PRNGR] if you will.

Meanwhile, I would side with Barrack because some ccTLDs predict that their economic/financial standing might be affected by the COVID crisis. But, again, there is a certain lag, obviously, at least until the end of this year, so it remains to be seen they are seriously impacted.

Overall, I would say that the major issue of ccTLDs in the region were really concerned about was the development of temporary policies which I'm afraid are going to permanent ones. These policies mostly concern those urgent measures to be taken to counter effects of the COVID crisis. [inaudible].

NICK WENBAN-SMITH: Thank you. Touching on security has always been an issue. I guess it exacerbates that.

Moving on in the last five now minutes we've got, it's so bleak—the economic problems, the security problems, extra regulations, criminality—all these sorts of things—is there any silver lining to these dark clouds of problems and uncertainty and existential danger to ccTLDs?

Nacho, what are the good things about this which are going to come out—a crisis not going to waste, as Winston Churchill says.

NACHO AMADOZ: Can you hear me now?

NICK WENBAN-SMITH: Yes. That's perfect.

NACHO AMADOZ: Okay. Thanks. Well, actually there has been some interesting growth in registrations. Some of our members are really enthusiastic about this, and some others are more cautious because they say many, many small and medium business are going online and many of them are also closing. So maybe this great positive impact we're having during this month we'll see, next year, fall down. So there are some mixed opinions within our members.

We had, in April, we had 24% growth year on year, and this month we had 64%. So that's a really good number.

NICK WENBAN-SMITH: Wow. 64%. Wow.

NACHO AMADOZ: Yeah. [inaudible]. We don't have all the numbers yet, so we might be a little more—

NICK WENBAN-SMITH: My goodness. That's incredible.

NACHO AMADOZ: Yeah.

NICK WENBAN-SMITH: Wow. So it's not all bad, is it?

NACHO AMADOZ: No. So [inaudible]—sorry.

NICK WENBAN-SMITH: I was going to say we only got a couple minutes left, so I just wanted to give all the panelists to talk about the potential positive side effects of the terrible crisis we're experiencing.

Barrack, any positive messages from the African region?

BARRACK OTIENO: Yes. Thank you very much. The COVID-19 pandemic has really brought great awareness on the role of the DNS and, by extension, ccTLDs and gTLDs, if I may. I believe, going forward, we are going to see a marked growth based on the increased information that is being relayed to the public, encouraging them to go online and, basically, the awareness of governments that there's a need to do more business online for the economy to be sustained. So I think all this is a silver lining, especially for the economy. I want to believe that, by the time we get over the peak in most of our countries, we should see a remarkable increase in

consumer data using DNS-related products and services. Thank you very much.

NICK WENBAN-SMITH: Thank you very much. That's really positive to hear.

Leonid, I'll give you 30 seconds on the silver linings for the Asia-Pacific if there's anything new.

LEONID TODOROV: Thank you. The growing role of ccTLDs in the local DNS ecosystem is probably the most important thing, coupled with some group in registrations. Thank you.

NICK WENBAN-SMITH: Very good. Peter, last but not least, the positives?

PETER VAN ROSTE: I think four points. First of all, proving that the DNS keeps working is quite important. Shouldn't forget that. Secondly, it's a good test for cooperation with local authorities/law enforcement/consumer protection/health authorities. Thirdly, the lessons learned from this exercise, whether it's internal-procedure-wise, cooperation with other ccTLDs, TLDs, and ICANN, will be very valuable in the future. I also believe that this is a good start for healthy data and accurate data-sharing discussion within our industry.

Just one short sales pitch here. There's a dynamic coalition forming on data and trust in the context of IGF. If anybody is interested in learning more, then please contact me.

NICK WENBAN-SMITH: Thank you very much. A really genuine thanks to all of the panelists for contributing to this. I think it's been a super interesting area. I think we've heard a huge amount of things from all around the world. Certainly, the responses have not been uniform. It's been very diverse, as you would expect anyway in the ccTLDs in terms of the African experience around the impact on access. The Asia-Pacific is much more of government agencies and is taking a bit of time to respond. The truth that we've heard that, despite all of the noise about the problems, the actual numbers of problematic registrations are vanishingly small in context is something that's a really important message to keep in mind.

Finally, actually it has opened up a lot of new areas for dialogue and, if anything, made us more relevant and important going forwards. That must only be a good thing for us.

I'd like to thank everybody very much, and I'll just hand it back to Alejandra for the last minute.

ALEJANDRA REYNOSO: Thank you very much, Nick. Well, I want to thank all of our panelists and presenters for their time and collaboration, as well as all ICANN staff who have supported this session. Great job, everyone.

Before the close of this session, I have a few announcements. Today's slide decks will be available in the public schedule after the session. Tomorrow, Thursday the 25th of June, is the session of Q&A with ccNSO-appointed Board members at 8:30 UTC. So don't miss it. And the Meetings Programme Committee wants to hear from you. Please feel in the satisfaction survey that will be circulated tomorrow by e-mail.

Thank you all for your attendance. This session is closed. Bye-bye.

[END OF TRANSCRIPTION]