ICANN77 | PF – ccNSO: Legislative initiatives affecting ccTLDs
Thursday, June 15 2023 – 10:45 to 12:15 DCA

CLAUDIA RUIZ: Hello and welcome to the ccNSO legislative initiatives affecting ccTLDs session. My name is Claudia Ruiz, and I along with my colleagues, Bart Boswinkel and Kimberly Carlson, are the remote participation managers for this session. Please note that this session is being recorded and is governed by the ICANN expected standards of behavior. During this session, questions or comments submitted in chat will only be will only be read aloud, if put in the proper form, as I have noticed in the chat. I will read questions and comments aloud during the time set by the moderator or chair of this session. The interpretation for this session will include Spanish, French, and Arabic. Click on the interpretation icon in Zoom and select the language you will listen to during this session. If you wish to speak, please raise your hand in the Zoom room. And once the session facilitator calls upon your name, kindly unmute your microphone and take the floor. Before speaking, ensure you have selected the language you will speak from the interpretation menu. Please state your name for the record and the language you will speak if speaking a language other than English. When speaking, be sure to mute all other devices and notifications. Please speak clearly and at a reasonable pace to allow for accurate interpretation. This session includes automated real-time transcription. Please note, this transcription is not official or authoritative. To view the real-time transcription, click on the closed caption button in the Zoom toolbar. To ensure transparency of

participation in ICANN's multi-stakeholder model, we ask that you sign into Zoom sessions using your full name. For example, first name and last name or surname. You may be removed from the session if you do not sign in using your full name. Thank you. And with that, I will now hand the floor over to Annaliese Williams. Thank you.

ANNALIESE WILLIAMS: Thank you. Welcome, everybody, and thank you for joining us for this ccNSO news session, which is being organized by the ccNSO's Internet Governance Liaison Committee. My name is Annaliese Williams. I'm from the .au domain administration, and I'm also the chair of the IGLC. Today's news session is on legislative initiatives relating to cybersecurity and how they affect ccTLDs. We have speakers today from Canada, Vanuatu, Mozambique, Costa Rica and Slovenia. Each of our presenters has been asked to consider the cybersecurity legislative initiatives that impact on their ccTLD or their country or region, and whether their ccTLD is able to influence the development or implementation of that legislation, and what, if anything, they've done to manage the impact of these initiatives. Each of our speakers will have 15 minutes for their presentation, which includes time for audience questions. So we'll be keeping to that time so that each speaker gets their allocated time. But if there is any additional time at the end of the session, I'll open the floor for further comments or questions. And just another reminder that we have interpretation available for this session. So can I ask each of our speakers to speak slowly and clearly so the interpreters can keep up? So now let me introduce our first speaker is Sabrina Wilkinson. Sabrina is the policy and program manager at the Canadian Internet Registry Authority. She holds a PhD in media and

communications and has led a range of research projects in the areas of digital policy, journalism and gender. Over to you. Thanks, Sabrina.

SABRINA WILKINSON: Thanks, Annaliese. So it's very nice to be with you all here today. Today, I'd like to talk to you about CIRA's views and engagement with a major piece of domestic federal cybersecurity legislation or proposed piece of domestic federal cybersecurity legislation called Bill C-26 that's currently moving through Canada's legislative process. In particular, I'll be focusing on the second part of the bill. Next slide, please.

So in this presentation today, I'd like to do three key things. First, I'd like to tell you about what exactly is being proposed in the second part of the bill that CIRA is engaging with. I'd like to tell you about how CIRA has engaged with this dialogue around Bill C-26 to date, both in developing public policy positions and advocating for them. And I'd also like to touch on how CIRA plans to continue its engagements on an ongoing basis. Next slide, please.

So Bill C-26 is made up of two key parts. I'm going to focus on the second part because this is the element of the bill that CIRA is engaging with. And in short, what this proposed law would do, which if it were enacted, would be called the Critical Cyber Systems Protection Act. What it would do is it would first apply to federally regulated operators in four identified critical infrastructure sectors, which are telecom, banking, energy, and transportation. And it would allow the government to place requirements on specific designated operators within these four federally regulated sectors to ensure that they take certain steps around cybersecurity, develop cybersecurity programs, for instance,

report on certain cybersecurity events that may occur, and keep specific records in the realm of cybersecurity as well. The proposed law would also establish regulations, give the government the power to order designated operators underneath these four sectors to take certain steps to address a cyber incident, for example. And it also lays out a number of enforcement powers that the government would have in cases where these steps aren't taken or these requirements are not fulfilled. Next slide, please.

So why does Bill C-26 matter to CIRA? Why do we care about Bill C-26? And why are we engaging in this ongoing policy dialogue? A few different reasons. One, Bill C-26 has the potential, and part two has the potential to capture a wide range of operators beyond those that are currently outlined in the bill. In addition, the objectives of part two are aligned with... So the objectives of the proposed law, which are to broadly raise the baseline level of cybersecurity across critical infrastructure, is very much an objective that's aligned with CIRA's mission to build a trusted internet for Canadians.

There's also an opportunity for CIRA to engage to improve the bill. So not only is the bill relevant to us as an operator aligned with our mission of building a trusted internet, but we see there being a space for us to really have a meaningful, positive impact on certain provisions within the bill. And being located in Ottawa, which is Canada's capital, we're also geographically quite close to the spaces where decisions about how the bill should be amended or developed are happening right now.

Finally, we also see engagement in the policy dialogue around Bill C-26 as a thought leadership as well as a product awareness opportunity. By

that, I mean that it's a space where CIRA can meaningfully contribute as a technical operator with expertise relevant to cybersecurity and other related issues that are outlined in the bill. And it's also an opportunity for showcasing our products as a cybersecurity provider as well. Next slide. Thank you.

So in reviewing the bill, CIRA came across a number of concerns. So while we broadly are aligned with the objectives outlined in Part 2 of Bill C-26, there are nonetheless areas where we see there being space for improvement. And this is the basis on which we are engaging, or these are the policy positions we're outlining when we're in meetings or having discussions around Part 2 of Bill C-26. At a very high level, these concerns relate to three key theme areas or issues. So we have concerns around oversight.

As I mentioned earlier, Bill C-26 would grant the government quite expansive powers, in particular in its enablement of the government, in it allowing the government to order designated operators under the bill to take certain steps in what would likely be emergency situations. There are some existing oversight provisions around that power, but to some degree they are limited.

CIRA also has concerns around information sharing, given the amount of information that would be collected under the bill or under the law, or if it were to become law, and the extent to which that information would be shared among a wide range of parties. And finally, CIRA has some concerns around transparency. So certainly we recognize that in matters of cybersecurity, secrecy to some degree is necessary and important. However, we believe that there is space for additional

transparency that would give information to Canadians as well as designated operators around how, in particular, those directions to designated operators are being used. Next slide, please.

So in response to these three concerns, we're putting forward three related recommendations. At a very high level in our advocacy or engagement around Bill C-26, we're asking for an additional oversight mechanism to be added to that process of issuing cybersecurity directions. We're suggesting that information sharing underneath this proposed law should be limited to specific purposes only, because in our view there is some ambiguity around the extent to which information collected under the bill can be shared. And finally, we are advocating for annual transparency reports to be published that would provide Canadians as well as designated operators with more information about how the directions that the government can use in certain instances are actually being used. Next slide, please.

So we have these three recommendations, which flow into a series of proposed legislative amendments, and we have these various concerns. How exactly have we been engaging with those making decisions about how the bill should be developed or amended in the midst of the legislative process, and who have we been engaging with, and to what extent has this been successful?

Broadly, we've had three kind of key activities or areas of engagement, I would say. First, we've had a range of meetings with decision makers and other stakeholders. So we've met with other actors who are involved in this dialogue about Bill C-26 and how it should be improved. We've met with decision makers or those supporting decision makers,

such as political staff. We've also met with a number of high-ranking public servants who are involved in the development of this, who were involved in the development of this piece of legislation, and who are working broadly in the areas of cybersecurity and critical infrastructure.

We've also engaged publicly in spaces such as this one, as well as in a public panel at a major Canadian telecommunications conference, where we were able to both share our views as CIRA, and also engage with others who are engaging in this debate as well, and who hold expertise in this area. And we've also done some public writing around our policy views, and the extent to which we think they should be incorporated into the law. Next slide, please.

So, how do we plan to continue engagement as this bill continues to move through the legislative process? So, right now, the bill is in what's called the committee stage. So, the bill is waiting to be reviewed by a group of parliamentarians who study matters of public safety and national security. So, we will be continuing to closely monitor the bill's progress as it kind of moves into this committee stage and begins being reviewed by these parliamentarians, as well as other expert witnesses. We'll continue to meet with decision makers and stakeholders who are involved in this debate to share CIRA's views, get a better sense of what other parties are thinking and what's driving their motivations and insights. And we will also continue to publicly advocate for CIRA's views on, in particular, the second part of Bill C-26 in public fora, such as international spaces, such as this one, as well as in domestic venues as well.

So, I hope today I've given you some sense of, a little bit about what this law looks like, or this proposed law looks like at a high level, how CIRA is engaged to date and what exactly that's looked like, and also how we plan to continue engagement ongoing. I'd be happy to answer any questions.

ANNELIESE WILLIAMS: Thanks very much, Sabrina. Are there any questions for Sabrina? Yes, please, Sean.

SEAN COPELAND: Of course, I would have a question for you. So, Sean Copeland for the record, NICVI, but speaking as a Canadian citizen, how has your position on the oversight been received?

SABRINA WILKINSON: Thank you, Sean. I would say all of our recommendations have been positively received by those decision makers, as well as stakeholders that we've met with. With respect to the oversight mechanism in particular, we've tried very hard to strike that balance between providing an additional level of oversight, while also maintaining a level of speed and secrecy, because we recognize that in matters of public safety and national security, that's crucial. So, I think and hope that we've struck that right balance, and I think the positive feedback we've received suggests that that might be the case. Thank you.

ANNELIESE WILLIAMS: Thanks, Sabrina. Any other questions? I don't think I see any, so we might go on to our next speaker. So, our next speaker is Norman Warputt. Norman is the ICT and Internet Governance Manager at Vanuatu's Telecommunications, Radio Communications and Broadcasting Regulator. Go ahead, please, Norman.

NORMAN WARPUTT: Thank you, and once again, good morning, everyone in the room. Good night and good evening to our remote participants. My name is Norman Warputt, and I'm the ICT Manager for the Telecommunications Authority in Vanuatu, which is also the delegated holder of the .vu ccTLD. Next slide, please.

So, my presentation this morning, I will discuss mainly some initiatives that we have worked in collaboration with the Vanuatu government, and also our role as the .vu ccTLD Manager and Administrator. So, basically, briefly about the Telecommunications Authority in Vanuatu. It is a statutory body operating independently from the government. So, we don't have any board of directors, or we don't have any commission. We have the regulator and the staff. So, all the decisions are entirely with the regulator. So, we do have general functions and powers to regulate the telecommunications sector, and also the broadcasting sector. The regulator reports to the Prime Minister, and also advises the government on ICT policies from a national interest. Next slide, please.

So, .vu is our country's top-level domain namespace, and it is being managed by the Office of the Telecom Regulator. Initially, our ccTLD was managed by our telecom company way back in the 1990s. So, when

the Office of the Regulator established, the law requires the Office of the Regulator to manage and administrate this resource. So, we have a transition from the telecom Vanuatu, started in 2017, and we successfully completed that in January 2020. Next slide, please.

So, from the internet security perspective, when we are planning for the transition, the Office of the Regulator approved GoDaddy as the registry operator for .vu ccTLD. So, the registry operator starts to provide the service that meets ICANN and international best practices. We developed a few policies for our ccTLD, and also we developed a domain name regulation that was finalized in 2016. Currently, we have 34 international registrars and 5 local registrars, and so far they are complying with the required international security standards set by the registry operator. Next slide, please.

The Office of the Regulator also supports and assists the government in drafting the Cybercrime Act. We do have a consumer protection regulation that allows us to inform consumers about the risk of internet security and child protection. So, the Act has been finalized, and it is passed with our national parliament, and it's [discussed] in 2021. Next slide, please.

So, one of the initiatives that we work with the government in collaboration with the Office of the Government Chief Information Officer, we established our CERT, our Computer Emergency Response Team. So, the Office has now established in 2018, and it's still in operation currently. Next slide, please.

Another initiative is the establishment of the Vanuatu Internet Governance. We also assist the government, and that is just after

Vanuatu hosted the APRIGF here in 2018. So, this Office is basically a multi-stakeholder platform that facilitates discussions of public policy and issues. So, it is supported by the Office of the Regulator and the Government Chief Information Officer. Next slide, please.

We've also developed a SIM registration regulation. So, this basically is an instruction from the National Disaster Management Office, and it is based on the Council of Ministers decision for us to have a regulation to register all SIM cards and assign to a valid national identity. So, that regulation has been finalized. And it's now in the market. All the ISPs and especially the two main mobile companies, they use that for SIM card registration. And this is basically a cybersecurity measure, and it adds value to cybersecurity initiatives in the country. Next slide, please.

We have a few national legislative initiatives that we've also assisted the government with, in collaboration with the Office of the Government Chief Information Officer. At the moment, we're in the process to submit these bills to our national parliament, and hopefully in November this year, we will have some update on that. However, this national legislative, we have the harmful digital communication bill, data protection and privacy bill, and the talent and protection. So, these are the cybersecurity measures, which also adds value to our national cybersecurity initiatives in the country. Next slide, please.

Again, we've involved a lot on the community awareness. We do have a consumer protection regulation, and also the SIM registration regulation. So, it's important to inform our users, especially on the benefits and the risk of using Internet, and the relevance of this regulation, how it will impact the consumer. So, this is part of our

awareness program throughout the year. And we've also participated with schools, communities, and in collaboration with the Vanuatu [IGF] Internet Governance, and other stakeholders to promote awareness across the country. Next slide, please.

I think that's all I have. Thank you. Thank you, everyone, for listening.

ANNELIESE WILLIAMS: Thank you, Norman. Are there any questions for Norman? I might ask one, Norman, if you don't mind. I know that you weren't directly responsible as the regulator, but Vanuatu quite recently had a very major cyber attack. Are you able to offer any reflections on how that impacted on your office?

NORMAN WARPUTT: Thank you for the question. Yes, basically, what happened—I don't have any detailed information to the ransomware attack last year. However, it's a ransomware attack, and I think the hackers basically hacked one of the [inaudible] servers. So, the team from the government has to shut down the server to take the hacker away, and then they locked down the system. But basically, from a .vu ccTLD perspective, we don't have any great impact on that. However, the government has to disconnect a lot of services online just to ensure that they can rebuild the server and restore all the data from the backup.

So, I think the impact that I've seen is the payment process, the [border] controls, the websites, the email. The government has to take those

services down in order to fix this issue. I think that's all I can provide an update on that. Thank you.

ANNELIESE WILLIAMS: Thank you, Norman. Any other questions? Yes, I see Angela, please.

ANGELA: Good morning, everyone. So, Angela, for the record, by the way, I wanted to ask about if there are any specific regulations that speak to online radios, right? So, usually, you'd have that in the broadcasting, maybe policies and stuff like that, but do you treat it differently because now you have a radio that's running on a domain space? Would then that mean the ccTLD policies that speak to abuse also speak to this radio content that's running on a domain platform? Thank you.

NORMAN WARPUTT. Thank you. So, the office of the regulator, from a content perspective, we don't regulate the content. We only regulate the telecom service and we monitor the market, but we don't regulate any content either from any content website or anything that comes up from the broadcasting. We don't regulate content. I hope I answered your question. Thank you.

ANNELIESE WILLIAMS: Thanks, Norman. Are there any other questions? I don't see any in the room and I don't think there are any online. So, we may move now to our next speaker who is joining us online remotely. We have Lourino Chemane. Lourino is currently chair of Mozambique's ICT regulator, the

National Institute of ICT. Previously, he was ICT advisor to the Minister of Science and Technology and Higher Education, and he has also previously been the CEO of Mozambique Research and Education Network. Go ahead, please, Lourino. Thank you.

LOURINO CHEMANE: Thank you for the opportunity given to us. My name is Lourino Chemane from Mozambique to share what we are doing in Mozambique in the field of cybersecurity and the legislative initiative related to ccTLD. We represent the National Institute of Information Communication Technology. That's the regulator of the digital service in Mozambique. Next slide, please.

These are the topics that will be covering. A brief introduction, INTIC's mandate and competence, management of the Mozambique ccTLD, the approved legislation, the national cybersecurity policy and strategy, the follow-up actions, development of the new legal frameworks, and a brief conclusion. Next slide, please.

So, INTIC has been created by decree in 2011, but that decree has been revised in 2020. That designates INTIC as the ICT regulator in Mozambique. It's a national public institute endowed with legal personality and administrative autonomy as the ICT regulator in the country. And it's supervised by the minister who oversees the area of information and communication technology, and currently in the current government is the Minister of Science, Technology and Higher Education. Next slide, please.

As part of INTIC mandate, it's included the development of proposal for policy standards and regulation that ensure the security and integrity of IT systems and operation against possible abuse and violation. And also state explicitly that the INTIC has to ensure internet governance in Mozambique. Next slide, please.

One of the areas of the mandate that's specific is to ensure the operation and management of the Mozambique ccTLD, that's the .mz domain, besides working also in other areas like the digital certification of Mozambique, and also the registration of the digital operators and the intermediary service provider. Next slide, please.

Within the scope of the ccTLD, in particular the .mz domain, I would like to share a brief history. The .mz has been established in 2015, and it has been operated by Eduardo Mondlane University, an academic institution that has registered itself. But with the approval of the electronic transaction law in 2017, INTIC has been established as the entity responsible for the management of the Mozambique ccTLD. And we are now in the process of working with the university to transfer part of the roles and responsibilities of the ccTLD to INTIC. But we are leaving all the technical operation to the university because of their history in operating the .mz domain in Mozambique. Next slide, please.

There are many competencies of INTIC in the law, but one of them was to give clear instruction for the development of the regulation of the use of the .mz domain. We have done that work, and this regulation has been approved in 2020 that indicated the process and the procedure for the management of .mz domain. We are the member of SADC, and that's part of the SADC and the ministerial meetings of SADC. Ministers

responsible for ICTs have been attending. There are clear indications that the member states have to work toward implementing the DNSSEC in their respective countries, and we in Mozambique are doing that also. Next slide, please.

We are also following the national development side, the national, and all the international. I would like to share the Malabo Convention, the African Union Convention related to cybersecurity and data protection, and that Mozambique is one of the countries that is signatory to that convention. And that we are following closely the work by the United Nations in the preparation of the proposal of the United Nations Convention against the use of ICTs for criminal purpose. And we are also working towards acceding to the Budapest Convention as part of the international exercise that we're doing. Next slide, please.

On the specific cybersecurity action, the government of Mozambique has approved the National Cybersecurity Policy and Strategy in 2021, and it's identified the coordination mechanism for the governance of cybersecurity. And in the structure that I'm showing here, that committee is chaired by the minister who oversees the ICTs and indeed has the role as technical secretary. And the members of this cybersecurity committee include the law enforcement agencies, the justice department, the ICT regulator, the telecommunication regulator, the academia, the national CSIRT, civil society, and private sector. So we follow the multi-stakeholder approach in the establishment of this commission to oversight the process of the implementation of cybersecurity in the country. Next slide, please.

The National Cybersecurity Strategy identifies 25 initiatives divided by seven areas. I'm sharing here in red the areas that are related to this topic that we are covering today, which is the developed guidelines, legal and regulatory instruments for the protection of critical infrastructure, strengthening the legal framework on cybersecurity, and establish the Center for Internet Traffic Research and Analysis. Beside also establishing the national CSIRT and also the National CSIRT Network and mapping of critical information infrastructure. We believe that these activities somehow are related with the ccTLD and cybersecurity because of the role of the internet in the operation of the cybersecurity of the critical infrastructure. Next slide, please.

In terms of follow-up development, we would like to share the work in progress in the preparation of laws. So we're preparing the cybersecurity law, the data protection law, and also the cybercrime law. And we're in the process of working on the regulation of registration and licensing of intermediary service provider and the digital platform operators. And we're listing also here other regulations to be developed within the coming years, and that these are related with the ccTLD work when it comes to cybersecurity. Next slide, please.

In terms of the development of the legal framework, we believe that we do have a major role to play because as the ICT regulator, we are the one tasked with preparing the proposals of laws to submit so that they can follow the legislative process so we can influence the regulation and other normative instruments related to ccTLD. We can propose change of the normative instruments related to ccTLD and cybersecurity. And as ccTLD manager, INTIC is responsible for managing and administering the .mz domain and also provide name

resolution services, maintain the critical infrastructure needed to complete the work of the DNS queries, and provide registration services to registrars, which can include creating or cancelling domain names and updating a name server. We believe also that in this sphere, INTIC has a significant role to play in aligning the cybersecurity normative instruments, also the technical work of implementing cybersecurity mechanism related to DNS or to the ccTLD. Next slide, please.

This is the last slide, and we believe that the review of the new domain registration policies under the Mozambique ccTLD will include security aspects. We'll be working toward the implementation of the ccTLD security infrastructure with emphasis on DNSSEC. We'll comply with the recommendation of the intermediary service provider as soon as the new cybersecurity law and the regulation for the registration of intermediary service providers is approved. We'll be also working towards complying with the Budapest Convention as soon as the accession process is completed. We'll comply with the ICANN policies for ccTLD and other TLDs and other internet management related aspects. Next slide, please.

This is the last slide of my presentation. Thank you for your attention and sorry for being a bit faster for the technical team supporting the translation. Thank you.

ANNELIESE WILLIAMS: Thank you very much, Lourino. Any questions for Lourino? Yes, please, Anil.

ANIL JAIN: Thank you. INTIC is acting as a regulator and also acting as a ccTLD manager. Don't you feel that these are conflicting roles with each other?

LOURINO CHEMANE: Thank you for this question. In fact, we are not only the ICT regulator. We are also working as the cybersecurity authority. We are also working as the responsibility of ccTLD. In general, we have the task of overseeing the internet development in the country. So the role of the regulator of the digital service is one of the roles, but it's not the only one.

You are asking if they are not conflicting interests. We believe that there are governance mechanisms that are being established with the participation of all the stakeholders in the country that can help us in the oversight of the activities undertaken by INTIC. We are a developing country with considerable limitations in terms of financial resources, and we are not in a position to have multiple entities, depending on the new areas related to the digital technologies development.

For example, so far, we do have two regulators, one for the telecommunications regulator and INTIC, that is the ICT regulator, including these other areas that I've just mentioned.

ANNELIESE WILLIAMS: Thanks, Lourino. Any other questions? I don't see any in the room. There are none in the Zoom. So we may move on to our next speaker now. Thank you. So our next speaker is Rosalia Morales. She's the executive director of NIC Costa Rica, the .CR ccTLD. Rosalia has been involved with .CR since 2012. She's led projects related to internet

governance, IXPs, cybersecurity, internet infrastructure, and internet policy, and she's previously a member of the LACNIC board. She's been involved in working groups in the ccNSO and ICANN, LACTLD, and Costa Rica's local IGF. Rosalia, please. Hello, everyone. I'm going to give an overview of our cybersecurity initiatives and how cybersecurity legislation has affected our ccTLD. Next slide, please.

So first, I'll provide an overview of what cybersecurity means in our ccTLD, following by legislature overall. Next slide, please. So for .CR, cybersecurity is a key issue of interest. We've been working in cybersecurity intensely for the last 12 years. And by that, I mean that we're part of the national CSIRT in Costa Rica. We're part of the board. We have worked together with the government, with ISPs and other organizations, key organizations in the infrastructure of Costa Rica, in providing workshops with local and international agencies. And we've also worked in different international cooperation projects to help out with cybersecurity infrastructure in the country.

As I mentioned, we're part of the national CSIRT. We're actually the organization that provided the first equipment for a government CSIRT. So we started with the trainings and with the technical capabilities for the national government to start the cybersecurity initiatives locally. We organized trainings and awareness programs for schools, for universities, and for the technical community in Costa Rica. Overall, our policies, just as many of us have mentioned in previous presentations, we're not responsible for content. And for any kind of change we can make for a domain, we would need a court order to make any changes when it comes to if any of our domains are part of a cybersecurity issue or case locally or internationally. Next slide, please.

So currently in Costa Rica, we have ratified the Budapest Convention in 2017 by our local Congress. However, currently there is a delay in other complementary legislation that needs to be passed in order for this convention to actually work appropriately or have a rapid response from our local agencies. One of the main issues is the virtual undercover agent. That's a law that needs to be created and passed. At this point, it's only an idea and a discussion that is being held in Costa Rica, but it hasn't been ratified. And the second one is digital evidence. There's a protocol for our local authorities as to how to treat digital evidence. But when it comes to the Budapest Convention, it actually lacks the official legislature stamp that it needs for the process to happen accordingly and as fast as needed by the international authorities.

Second, we have ratified, I'm sorry, we have accepted the second additional protocol of the Budapest Convention in 2022. It has not been ratified in Congress since I understand there's still a couple of countries that need to adhere to this amendment in order for that to be passed to our local assembly. So we're just following the discussions. And one of them is the impact that this amendment would have in the WHOIS, but we're still waiting for the legislature to be actually passed and ratified. And we're counting on our local European counterparts to do an amazing job and help us out with that.

Second, there's the cyber crime law, the first law that was passed in Costa Rica directly affecting how cybersecurity issues were managed locally. And that was passed in 2013. It has actually helped us. It did not affect our policies or our operations. It has actually helped us because it provided a path for our local clients as to how to proceed if they have any conflict. In the past, it was pretty much a gray area and there was

not much they could do. And now there's actually a clear path as to how they can access the local authorities and do something about cybersecurity crime that might be happening in their domains. And lastly, there's a UN cyber crime treaty that is currently being discussed in the United Nations. Costa Rica has taken a very neutral stance. And as such, we're just watching and seeing what happens. So far, we're just spectators and hoping to see what comes out of those discussions. Next slide, please.

There are other initiatives that have affected the cybersecurity space locally and also how we operate as a ccTLD, which is not necessarily a law that has been passed by Congress, but that affects our operations. As I mentioned, the National CSIRT is something that we have been part of throughout time since its creation. And currently, there has been this in the last semester, a big interest in strengthening the CSIRT and the equipment that it has, the training and the staff. And as well as a local training of national agencies and all those other organizations such as .CR that provide stability for the Internet in Costa Rica. And the U.S. government has provided significant funding to our government to strengthen cybersecurity. And we are part of the organizations that are helping out the government to carry out intense trainings in cybersecurity.

These trainings have not started. However, we have been asked to be part of it, and we're waiting to see what happens. It's a project that is supposed to last about five years. So the cybersecurity interest or the focus of cybersecurity may have on a government and usually even the role that we play together with the government depends on the government in charge at that particular point in time. It's not stable.

Some governments are extremely involved. Others are not. In this case, they're pretty involved. Since last year, Costa Rica suffered some important hacking incidents of our treasury and our health care service. For more than six months, they were hacked, and it created a national crisis. So since then, that's why we have received international help, and it has become a point of importance for current government and as such of our organization.

Then there's also a cybersecurity strategy that was created, and it was finished last year in 2022. This is a strategy that was created by the Ministry of Technology, Science, and Telecommunications together with the Organization of American States, the OAS. This cybersecurity strategy did not impact us, our policies, or work day to day directly. We were part of the discussions and the feedback sessions of this strategy. Overall, it's extremely broad, and this is an effort the OAS made in different countries throughout the region. So it's very similar to other strategies that the OAS carried out in other countries. So it doesn't necessarily apply directly to absolutely our specific reality of our country. It's extremely broad. So that did not affect how we operate. We're actually part of, as I mentioned, of the feedback sessions.

Currently, there's a law being passed to create a cybersecurity agency. This agency has become more of a discussion and may have an impact on our ccTLD and our operations, and overall, how data is managed in the country. It has not been ratified by Congress, and it does not seem like it will have the approval at this point, but it could change. Discussions in Congress change dramatically. As such, the law can change. Usually, when the discussions take place, they may add or delete amendments, and we are just watching and seeing what

happens to make sure that it does not affect our operations in a negative way. And if there is any way that we can actually help to improve it, we will definitely be available to provide feedback for this law. Because I think the law goes hand in hand with this new government's intention to improve and fasten the approval of cybersecurity legislation in Costa Rica. It's being pushed very quickly, and I think it still needs some debate. It hasn't been finished yet. Next slide, please.

So overall, the conclusions is that throughout this about 12 years of working closely with the different cybersecurity organizations in the country, we have created a strong relationship with the law enforcement agencies. And that has helped us have an open dialogue when it comes to different policies, projects, anything in the cybersecurity space that could affect our ccTLD. We're usually in intense communications with the agencies involved that has allowed us to be aware of what's going on and also make sure that it helps both parties or all parties involved.

Furthermore, cybersecurity is currently a key area of interest for our government and our ccTLD overall, which brings some risks. As I mentioned, there's some laws going on, which we still do not necessarily know what the end product will be. But we will be monitoring closely to make sure that it actually improves cybersecurity space and does not create some kind of danger or risk to the end user or ccTLD.

Overall, there's lots of work ahead. Costa Rica is just starting to work with cybersecurity legislation. As such, we have a lot to learn from other

ccTLDs, many of them in this panel, as to how to manage this creation of this new laws and how to learn from their experience and see how we can affect or improve our local cybersecurity legislature space so that we make sure that our ccTLDs are strengthened by this legislature and not the other way. And it also provides opportunities to work together with authorities from Costa Rica and abroad. It has given us the opportunity to even train our staff in the latest cybersecurity technologies and as such become the national trainers of other agencies locally and help out in that knowledge transfer and continuous effort to create a more stable and secure Internet in Costa Rica. Thank you.

ANNELIESE WILLIAMS: Thank you very much, Rosalia. Are there any questions for Rosalia? Olga, go ahead.

OLGA CAVALLI: Thank you. Thank you to all the presenters. Very, very interesting presentations. Thank you very much for that. And this is a question for Rosalia. I know you said this is a very brand new law that you're thinking about in Costa Rica. About this agency that you're thinking about, do you have any idea how it will fit into the bureaucratic structure of the government? It will depend directly on the presidency or how it will interact with other ministries of security, defense? And maybe you don't have that info, but just in case you have some. Thank you.

ROSALIA MORALES: Thank you, Olga. Yes, this law is actually created by the Ministry of Technology, Science and Telecommunication. Part of the issue with this law is that it's given the ministry some of the authority that the judicial system actually has and the Ministry of Justice actually has. For example, I understand it provides the ministry with the ability to talk to Interpol and exchange information, which is something the ministry does not necessarily currently have the staff, the capability or the experience to do that. So it's part of the dialogue that is going on. So I think it's confusing a little bit of the roles that each different ministry should have. And that has been part of the issue as to why the law does not move forward. But it's pushed by the Ministry of Science, Technology and Telecommunications.

ANNELIESE WILLIAMS: Thank you. Any other questions? I don't see any in the room and I don't see any in the Zoom. So we might, since we are, I think we have a couple of minutes, I was going to ask Rosalia a question, but I think I might address it to all panelists at the end. We were talking in the coffee break about how difficult it is to keep across all of the legislative initiatives that are emerging. So when we get to the end, I might ask all of the speakers just to help us understand how their registries are keeping across it all. But for now, we will just move to our last speaker. Our last speaker is Barbara Povse, the head of Slovenia's ccTLD and also the chair of the CENTR Board. Barbara has over 20 years' experience in management, business administration and EU policy and extensive experience in DNS, domain name business, privacy and information security. Barbara, go ahead, please.

BARBARA POVSE: Thank you, Anneliese. And good day to all of you. Thank you for a nice introduction. Yeah, I've got a lot of experience, as you can tell. I even remember when all the CCs were below the radar of any legislators. So, yeah, you wouldn't believe that we were not regulated at all. And definitely, these times have passed. So it's probably okay that I'm the last speaker. I was told that it's a running joke that the European best export product is being legislated. I'm not quite sure whether I should apologize or you will just take it.

So, first, I would like to thank you, Martha Moreira, who helped me with this presentation. So I'll be talking about how .SI and partially .PT are dealing with this enormous amount of legislation, mostly in cybersecurity, but also some other sectors. So thank you also to Polina from CENTR who checked, because I'm not a lawyer, that all the facts are correct. But all the possible mistakes that I'm going to make, these are completely mine. So Next slide, please.

You are probably familiar that not—all European countries are not facing just their national laws. I mean, but they are. Well, we are all under a big European legal framework. Here are the legal sources of union law, how they follow. And then if we go to the next slide, because I'm not planning to do a very detailed presentation on who is doing what in the European Union and who is responsible for which legislation and how all these decisions are making. Well, the result at the end is directives or regulations. But you can see from all these dots and arrows that it's quite complicated. And I have to admit that I'm still not very comfortable with each and every process that is going around.

But thankfully, I don't need to be. This is the great work that we get from CENTR, especially policy part of a small CENTR team. I don't think that from a perspective of a very small registry as we are, we would never be able not even to follow what's going on. Not to mention that influence would be out of question. Next slide, please.

So here is the list of EU cybersecurity acts that are relevant for CC and that are already in place. The first NIS directive, well, this was the start, a small step in a broad legislation flood in cybersecurity that followed and influenced ccTLD registries. We qualified at that time as providers of essential services. This is not exactly the same as critical services, but yeah, we got a lot of new responsibilities. And then now we have our NIS 2 with additional requirements. We are now in the phase where NIS 2 is being transposed to national legislation. And since NIS 1 was transposed in a way that was very different across countries, so now the legislators are trying to coordinate this. But just to mention how this will influence on our business. Well, mostly we talk about Article 21, about registrant verification, and there is a lot of unclear things still there. And then we have reporting obligations and so on and so on. There are also some guidelines issued by ENISA. Here is mentioned the security measures for TLD operators, but there is a new one exactly on registrant verification. These are non-binding, but still recommendations. And Next slide, please.

And here, well, this is not done yet. There is still some legislation in the field of cybersecurity that is being cooked, but not quite ready in the EU. But every day there are some changes. But as I already said, we luckily get thorough reports by CENTR staff that also include the relevance for

ccTLDs. And this is really extremely, extremely important. Next slide, please.

So how do we deal with all these initiatives? We try with centr and coordination, and we have a legal and regulatory working group where we coordinate and get informed what's going on. So we try to influence the coming legislation already when being prepared at the EU level. So we don't wait that the legislation is there, but when there is a first draft, we try to influence in the fields where it tackles us. So we do this with CENTR papers that you can also find on CENTR page, but also with a lot of meetings on EU level with lawmakers so that we try impact during all the phases of the process.

Then we as individual members, we try to inform our national MEPs so that they are aware of the new legislation getting ready and what are, for example, our recommendations for some changes. Well, here is also mentioned, CENTR recently established information sharing analysis centers, ISACs for TLDs. So this is also something very important for cybersecurity. And yeah, there is a lot of awareness, engagement and training going on the EU level. And next slide.

What about our national level? Yeah, main message, I think it should be that ccTLD should be proactive as much as possible if we want to influence the process. So, as I already said, we try to influence the process on EU level through national representatives, and then it gets to adoption of national legislation. We try to talk to every level of or to public, well, to ministries and all the lawmakers and try to educate them because they need to understand the basics, what some actions on the level of DNS actually mean. So I think we managed over the years,

maybe for Slovenia is easier. We are a very cute little country, and we know each other with two million. It's just two steps and you find the right person to talk to. But it also helps that we as a technical operator, but being more and more active on the policy field. So we try to bring technical and non-technical experts on the national level, trying to make them speak the same language. Next slide, please.

Maybe here I can mention what channels we used, all kinds of channels. So we participate at public debates. We use connections at ministries. We write some articles and blogs. We send emails. We phone people. And, of course, when there is a legislation and public consultation process, if not before, then we try to influence at that time. Sometimes we were quite successful, sometimes a little bit less. Maybe CPC implementation. This is the consumer protection cross-border regulation. Here we were very successful, communicated extremely well with the ministry responsible for implementation, and we got reasonable results.

We are not getting so good with NIS2 implementation. The national regulator is right now doing his own business and doesn't want to talk to anyone. But, yeah, let's hope this will change soon. Because I think it's extremely important that we talk to each other, because as cc we are as much interested in safe internet as our government is. We just need to make sure that regulation that we get, or legislation that we get, that is, well, applicable, and that we can do what is required for us, and that is the right action to be done. So sometimes there is not enough understanding there. Next slide, please.

So how does this impact our work? Yeah, we try to think forward, so we don't wait for legislation being really adopted. We try to prepare in advance, and, yeah, we are getting better in a crystal ball. So we follow the process since the beginning with a lot of help of CENTR. And since CENTR is a great community, we also learned from each other a lot and help each other and share resources, and this is really, yeah, especially for a small registry like us, this is of utmost importance.

What we did, we, even before NIS, we decided to get ISO 27001 certificate, and it turned out that was a very good decision, because then with, there is not so much work with NIS first. We have still some work to do on registration verification procedures. We are working on that. Yeah, compliance is the hot topic in Europe. It's in all fields, but this is really difficult to achieve, but we are working on that.

So what I meant by Brussels effect is Brussels is the leading force in cybersecurity legislation, and I think it's important that we get legislation, but we are not isolated. So the new requirements put a lot of strength and require, I mean, a lot of strength. Yeah, we get a lot of new obligation that costs the registry. We need to change our procedures. We need to find new people who can deal with new procedures. We need to put a lot of investment in our infrastructure. So this is getting difficult. Also, with that new requirements, the procedures for registration of ccTLD are getting more and more complicated for the end registrant. So does this mean that they will get fed up with this and they will go somewhere where it is easier to get a domain name? This can be a problem for staying, well, and competing with other CCs and also gTLDs. But on the other hand, I believe that we all want to rebuild trust in the internet. So at the end, I think we'll find

the right balance between the overburden and being too relaxed. So, yeah, we'll keep on working together because, yeah, we are a bunch of registries sharing the same burden more or less. So at least we can complain to each other. But no, but also we really share resources and it's helpful. So I think I'm done. Is that the last slide?

ANNELIESE WILLIAMS: Yes. Thank you, Barbara. I think that's a really important point you made about being forward-thinking and proactive and not waiting for things to just happen around you. Are there any questions for Barbara, please?

UGO AKIRI: Thank you. My name is Ugo Akiri. I used to be part of .ng. My question to Barbara is, when you say some European countries are being left behind, does it mean that a policy like the GDPR is now being adopted across board by all members of the EU?

BARBARA POVSE: Thank you for your question. No, that was a misunderstanding. No, it didn't mean that some European countries were being left behind. Then maybe I put it wrong. As I said, all mistakes are completely mine. No, it's the legislation is the same. I mean, the legal framework is completely the same for you or European members. So that's the same for all of us. What I thought or what I meant to say was that there is a lot of burden put on the European ccTLDs. That's how I meant that

European ccTLDs maybe are being pushed harder than others. That's what I meant.

ANNELIESE WILLIAMS: Thanks, Barbara. I think there was a question from here and there's also one in the Zoom room, but we'll go to the room first. Hi there.

OMAR CONTRERAS: My name is Omar Contreras. I'm with Identity Digital Inc. One thing I enjoyed and appreciated from your presentation kind of beginning to end was the collaboration. You kind of took into account, hey, we have limited resources and clearly working with Portugal and CENTR to sort of leverage what you do have to make the most of it. I'm curious if you have any recommendations for ccTLDs outside of Europe for having that same type of collaboration, thinking about Central America in particular or South America. How did you start those channels? How did you sort of find those areas to at least develop kind of resources together to then basically try to keep up? Do you have tips or tricks or suggestions you would be willing to share?

BARBARA POVSE: Thanks. Yeah, it's probably the situation is different in Europe because we share the same legal framework. So that makes it—even though that national implementation can vary, and in addition, we also have some national laws that are different. But still, there is a framework under which we all work together. But I think that when I was listening to all these presentations, it's the same in Costa Rica or Vanuatu. It's more or

less the same legislation is coming into place. So I would think that respective regional organization like for Europe is CENTR and all the others can probably offer some at least place for lawyers or policy people to meet and discuss where they can find common ground.

ANNELIESE WILLIAMS: Thanks, Barbara. We will take a question from the Zoom room now. Michele, go ahead, please.

MICHELE NEYLON: I'm actually in the room physically as well. Thank you. Good morning. Michele Neylon from Blacknight for the record and all that. Barbara, the regulatory burden, I mean, obviously, you're looking at it specifically from the registry's perspective. I'd be looking at it more from the registrar perspective and also trying to actually pay bills and make money in this space. Do you have any idea as to whether the European Commission and their friends have any understanding as to the level of competitive disadvantage that they're putting us all in with these regulatory burdens? Because, I mean, when I look at how the Americans are practically laughing at us every time they see these new things coming out, I mean, it's quite frustrating. Just to know, is there any light at the end of the tunnel or are we just going to be buried in paperwork?

BARBARA POVSE: I'm so sorry. I don't think I've got some good news, but this is what I wanted to say. Well, I really mentioned just the registries and it was not fair. It's true. All, not just registries, also the registrars and business in

general is facing these problems, staying competitive in this highly regulated space. And I don't think I got an answer. But I agree with you if that helps.

MICHELE NEYLON: Look, I'll take anything. When a registry agrees with me, I'm always happy.

ANNELIESE WILLIAMS: Thanks. Any other questions for Barbara? I see Bruce.

BRUCE TONKIN: Thanks, Anneliese. I'm curious, sort of, at the broader picture level, because it seems historically each cc has sort of independently within Europe come up with the rules that sort of work for its community. But now you're sort of talking at a regional level. And when I look at a lot of these changes, are they being sort of driven by broader changes across other areas of the economy and with sort of collateral damage? In other words, the security and critical infrastructure stuff has been built to deal with sort of major industry sectors. And then it's like, well, we'll add domain names to that as well. Or there's concern about privacy or there's concern about sort of know your customer rules. So, in other words, are they actually seeing a problem in the domain name industry itself? Or is it they're solving a bigger problem and then we're being rolled up into that problem?

BARBARA POVSE: You're asking me that they are trying to solve? You mean European Commission or what?

BRUCE TONKIN: Yeah, I mean, European Commission. In other words, what problem are they trying to solve?

BARBARA POVSE: I really believe that they are trying—but this is just guessing. I don't know. But the main purpose is rebuilding trust in the Internet. That this is the main goal. How do you do it? It's, yeah, I don't know.

BRUCE TONKIN: So that sounds like digital economy more broadly, is it? So they're trying to build trust in the digital economy of which we're part of that. Is that right? I'm asking the question.

BARBARA POVSE: Now you've lost me.

BRUCE TONKIN: So I'm just trying to understand what's the underlying driver behind all of this regulation in the domain name industry in Europe?

BARBARA POVSE: I'm not quite sure what—I'm probably not the right person to ask.

BART BOSWINKEL: Annaliese, this is Bart. That might be a very interesting question for the IGLC to dive into.

ANNELIESE WILLIAMS: We have many members from the European Union area, so we can add that one to the list too. Thanks, Bart. I did see a question over here. We've got Chris and then I see Jordan's hand in the Zoom room. Chris, go ahead.

CHRIS DISSPAIN: Thanks, Annaliese. A couple of things. So to answer Michele's question or at least give you my opinion about the answer to Michele's question, I actually don't think they care. I think they're just determined to legislate for what they didn't achieve through the multistakeholder model. And the fact that it happens to be targeted at ccTLDs in the main is simply because that's they don't have a choice, because if they're going to try and do stuff really can only legislate for ccTLDs. Although if you talk to some European regulators, they will tell you that as far as they're concerned, it applies to everybody. It doesn't, but they will tell you that it does.

And just for what it's worth, I ran a session last year at the European Summer School talking about fragmentation. And it was one of the panelists was, I won't give the names because it wouldn't be appropriate, but it was a very senior European Commission person who

said, yes, we are fragmenting the internet because you won't do what we want. So that is the background.

ANNELIESE WILLIAMS: Thanks, Chris. I think that one's a comment, but I'll go to Jordan next.

JORDAN CARTER: Thanks. I promise this is a question, Jordan Carter for the record. Barbara, do you think that the way the EU is doing regulation at such a high pace is consistent with its public support for the multistakeholder model?

BARBARA POVSE: You put me on the spot.

ANNELIESE WILLIAMS: But perhaps that's another one that we can take up as a group discussion. As Bart suggested, we can add this to the discussion for the committee as a whole, rather than putting you on the spot for personal views, Barbara. Are there any other last questions for Barbara or for any of our other speakers today? Michele.

MICHELE NEYLON: I just want to say thanks to you and to CENTR because you have been very, very helpful over the last year or so in helping us all to kind of try to navigate the bag of crazy, which is coming out from the European Commission. I mean, we can have this kind of backwards and forwards

and all that. I mean, the reality is that the European Commission is trying to regulate stuff because I think, as Chris said, they didn't get it elsewhere. So they're pushing it to pushing it where they can push it and they don't give a damn. And trying to navigate that is an uphill struggle. And I know that we're all going to be spending a lot of time worrying about NIS2 and some of these other things over the next while. And the rest of you outside the EU need to keep an eye open because your governments are probably going to start saying, oh, look what the Europeans did. Meanwhile, the Americans are laughing all the way to the bank. But thank you. The CENTR has been very helpful. It is really appreciated.

BARBARA POVSE: Thanks a lot. If a registrar is happy, then I'm happy.

ANNELIESE WILLIAMS: Well, on that note, I think we may bring things to a close. I think we've heard from all of our speakers today that cybersecurity is a key area of concern for all governments. There's a lot of legislation already in place and more down the pipeline. So it's great to have this opportunity to hear from each other and learn from each other. And please join with me to thank all of our speakers today. And I particularly wanted to acknowledge Norman and Lourino, who have just given their first presentations to the ccNSO. Thank you.

[END OF TRANSCRIPTION]