ICANN86 Seville | PF – ccNSO: ccTLD News Session (2 of 2)
Wednesday, June 10, 2026 – 14:45 to 16:00 CEST

CLAUDIA RUIZ

Hello, and welcome to the ccNSO: ccTLD News Session Part 2. My name is Claudia Ruiz, and I, along with my colleague, Joke Braeken, are the participation managers for this session. Please note that this session is being recorded and is governed by the ICANN Community Participant Code of Conduct, the ICANN Expected Standards of Behavior, and the ICANN Community Anti-Harassment Policy.

Please observe the following guidelines to participate in this session. They will be posted in the chat for your reference. During the session, questions or comments submitted in chat will be read aloud if put in the proper form as noted in the chat.

Interpretation for this session will include English, Spanish, and French. If you would like to speak during this session, please raise your hand in Zoom. When called upon, virtual participants will be given permission to unmute. On-site participants will use a physical microphone to speak. Please state your name for the record and the language you will speak if speaking a language other than English. And please speak at a reasonable pace to allow for accurate interpretation. Thank you. And with that, I will now

hand the floor over to Rocio de la Fuente, moderator for this session. Thank you.

ROCIO DE LA FUENTE

Thank you, Claudia. Good afternoon, everyone, and welcome to the ccTLD News Session, Part 2. My name is Rocio de la Fuente. I work for LACTLD, and I'll be the moderator of this session.

The purpose of this ccTLD News Session is to provide an opportunity for ccTLD managers from different regions to exchange developments, experiences, and challenges that might be of interest to the broader ccTLD and DNS communities. And today, we will have four presentations covering topics ranging from digital development initiatives, legislative changes to approaches related to DNS abuse mitigation.

Before I begin, I would like to introduce our speakers. We have Gitau Muraguri. He is the chief marketing officer at .ke. I apologize in advance if I'm not pronouncing the names correctly. We also have Irina Danelia. She's the deputy director of the Coordination Center for .ru ccTLD. Fatma Demirel from .tr. She's the .tr ccTLD coordinator at ITCA. And I have next to me, Idrissa Sarr. She is the .sn managing director. Welcome, everyone, and thank you for participating as speakers in this session.

As a reminder, each speaker will have 15 minutes for his and her presentation, including questions and answers. And for both speakers and participants, please make sure to have a headset

ready and available as some comments and presentations might be made in different languages and interpretation services will be available throughout the session.

With that, let us begin. I would like to give the floor to Gitau. I don't know if you can hear us, if you are online.

GITAU MURAGURI Yes, I can hear you very loud and clear.

ROCIO DE LA FUENTE Thank you. Welcome. And the floor is yours.

GITAU MURAGURI Thank you very much. A very good afternoon to all the delegates. My name is Gitau Muraguri. I am marketing manager at Kenyan Network Information Center, the registry for .ke. We'll be taking us through a quick presentation about Africa Rising and what's happening from the position of KENIC and what we are doing to take advantage of what's happening in the domain space in Africa from KENIC's perspective.

The presentation pretty much speaks about the impact and the case studies about the collaborations that we've been having with various organizations and institutions. And this is what's helping to scale our growth and we believe that applied elsewhere, this will also just help to really drive up the growth of domain and Internet uptake right across Africa. I'll be able to share with you all what's

been happening in our space in the last two to three years. That also just helps to paint a picture of what else can be able to be achieved in other organizations, with other registries right across Africa.

In Africa, right now you may be aware, Africa is really the youngest region where median age is about 19 years old. There's a mobile-ready population that is predominant in terms of population. The use and uptake of digital channels and digital mediums is really, really thriving and it continues to grow, and this has a potential to proceed for the next number of years.

The challenge that we face right now is no longer about Internet access, but it's also just about aligning the ecosystems that can be able now to support the growth and the uptake of domains, especially in our perspective, as well as the uptake of the Internet. If you notice the average age in Africa is way younger than what you would find in other parts of the world. So it's really a young population, very vibrant. A lot of us are looking for opportunities for growth, for innovation and exploration across many different fronts. So this is a huge opportunity that we need to take advantage of. I'll be able to share with you what Kenya has done and what can be applied right across the different registries in Africa.

What's happening in Kenya is we're using an infrastructure and we're turning this into adoption. That collaboration, if you look at the last three years, KENIC has been able to achieve more than 30% growth in terms of domain uptake. And how are we doing this? One

of the key initiatives has been to grow the number of active registrars who are helping to drive up domain awareness and domain uptake. From an internal perspective, we took on the challenge to ensure that information about domains is disseminated to our various audiences, and we're able to do this on a daily basis.

What we have done in Kenya is to ensure that right across the various digital and social platforms, we're sharing information about how to manage registries, how to register for domains for businesses and institutions and individuals to get online. And hence, we're trying to drive our audiences to ensure that, one, they have a digital presence and also to have a strong digital footprint, of course, with showing them what the eventual outcomes would be, either for their businesses or for the institutions or for their own personas. So we are adopting various strategies that are able to help us now drive this agenda for all the target audiences.

What's working for KENIC? We've realized the importance and the strength that comes across borders. I just like to point out one collaboration that we've had between KENIC, ICANN, and an organization called AFRALTI, through which we've managed to deliver training that helps African registries better manage their registries. We realized also that a lot of registries are much younger or much smaller than KENIC, but we have managed to bring them on board through the cooperation of ICANN and AFRALTI. And we've managed to bring more than 30 African countries into Kenya for lengthy training so that they can be able to manage both the

technical, as well as the operational aspects of registries so that they can be able to apply these learnings in their territories.

This is actually ongoing even right now. It has a three-phase process where they have online lessons and trainings which have been happening over time, and then they have a two-week session where they come into Kenya, and then we have deep immersions into registry operations and management.

We've also managed to run regional forums and technical exchanges. This is just how to build a stronger registry in governance capabilities. Maybe I can also just mention that because of the both regional and international collaborations and partnerships that we've had, KENIC managed to bring what you call Domain Summit Africa which attracted over 27 different nations, again, coming into Kenya to talk about all matters domains and the Internet. And also, in addition to that, we managed to bring in domain ecosystem players from the United States, from the UAE, from Africa, from Asia and India, and they all congregated in Kenya.

What's important for us is just that we have to continue building these partnerships and collaborations, because the shared strengths actually what helped to unlock a lot of opportunities and doors, not only for us but also for other institutions and organizations. For us, the drive to identify and strengthen different partnerships and collaborations is really, really at the core of our business.

The other thing that we've also just realized as KENIC and we're really pursuing is the impact of SMEs. Kenya currently has certain statistics, placed this at almost seven million small and micro enterprises. Officially, the number of businesses and such institutions that are being registered up to 150,000 each year.

One of the key initiatives that have been undertaken is to ensure that we have close partnerships and collaborations with the registration bodies, because then this will be able to unlock, not mandatory but close, to be able to include domain uptake during registration. Because this now would be able to unlock almost 150,000 new domains. This sort of partnerships is very critical and I believe the same would be able to apply across many different registries in Africa so that the partnerships with government or with institutions that are tasked with the formal registration of business and commercial enterprises would really unlock a huge domain market.

Currently, we have given ourselves a target of a million domains by 2030. Of course, it's going to be progressive. We're working hand in hand with other organizations just to be able to achieve this stretch target. We believe that is very doable. We're very intentional about the institutions, the personas who we are working with so that can be able to unlock the growth up to a million domains. The ambition is quite high and it's a stretch target but we believe that if this is applied right across the African registries would be able to get continental total domain database of 10 million even beyond by the year 2030. It is actually because we've seen it working. We are

certain that when these learnings are shared, we'll be able to get a lot of big wins within the ecosystem. For us, the reality is that it's no longer about competition, but it's more about collaboration, cooperation, and a lot of coordination between the various institutions and persons.

So what we would propose, not only for us but also right across the continent, is the pursuit of more collaborations, more partnerships, more strategic engagements that are able to unlock either different doors and different opportunities, so that we're able to grow not only within our borders but within the total African continent. There is a lot of opportunities, there's a lot of shared learning that can be able to be achieved. And I believe a lot of this become tangible and measurable outcomes. Every year until 2030, I believe we'll be able to register significant growth, not only in domains but also just in the depth and the penetration of Internet uptake for individuals and institutions alike.

That's my last slide. Our growth will not be defined by resources that are beneath our soil. It is defined by the networks that we continue to build, the partnerships that we nurture both locally as well as regionally. The lesson from us is very simple. When ecosystems collaborate, nations will transform. And when nations collaborate, continents will rise. I believe this is very much so for Africa. My challenge to the registries right across Africa is to look out for that one partnership or collaboration that you could

establish in the next 90 days. That would double your impact. Go after it with all you have and just do it. Thank you.

ROCIO DE LA FUENTE: Thank you very much. We have some additional minutes for one or two questions. Are there any questions in the room? Please raise your hand, or in the Zoom session. I'll give a few seconds.

I don't see any hands. Let me ask you a question from my side. You mentioned that partnerships are a key component of this initiative. Could you tell us more or share more details regarding how are you working together with all the ccTLDs in the African region in order to have this regional impact and the outcomes that are expected? Thank you.

GITAU MURAGURI: Thank you for your question. It's not only an example but it's something that's already happening. Kenya was the recipient of a grant from ICANN where we have partnered with another organization called AFRALTI which provides high-level training. We've managed to invite or call in a number of registries across Africa. We have a three-part program where they take registry operation and management training online. That happens in a period of about four weeks. And then they have an in-person training that happens in Kenya of a period of two weeks.

We've already done the first one. We did it in February. It was hugely successful. We had close to about 50 participants from right

across Africa. Phase two has been ongoing, the virtual training. And we have an in-person training that will be happening in July. And then we'll also have phase three.

These are the sort of collaborations that are helping to disseminate the information and training the upscaling for registries right across Africa. It is open to all registry operators across Africa and it is delivering a significant impact. Just giving that opportunity for more and more registry operators and persons to be able to upscale their skills, to improve on their skills.

ROCIO DE LA FUENTE: Thank you very much. If there are no further questions, we can move on with—Joke, yes?

JOKE BRAEKEN: Rocio, thank you very much. There's one question in the chat. I will read it out loud. Two questions, even. The first one, "Hello from Malaysia. When you mentioned integrated business registration with domain names, how does that work? Do you collaborate with Kenya's national business registrar?" This is a question from Muhamad Adian.

GITAU MURAGURI: Okay. I can take that. Yes, you're right. We are running a collaboration with what you call business registration services. This was informed by the fact that all businesses that operate normally would have to have their registration given by the

business registration service in Kenya. The partnership foresees or is working towards having the business registration process to include a domain acquisition through which also the registrant acquires an e-mail address, and hence any other communication that comes from the business registration service to the business owner has to go through that e-mail address. That then the domain, of course, it will have to be renewed on an annual basis, and hence that will also take care of issues like attrition or deletions. Yes, we will be working with business registration services, and this will help just in terms of sustainability and the long-term use of domains.

ROCIO DE LA FUENTE: Thank you very much, and also for flagging the question online. I think there's another one.

JOKE BRAEKEN: Thank you, Rocio. There's another question from Zerafinas Abu Hassan, asking, "Is it compulsory for businesses to register .ke?"

GITAU MURAGURI: Is this in relation to when we start off the partnership with business registration services? Because if it's prior to that, it is not mandatory that businesses get .ke. But of course, when we start off with BRS, then it is the most recommended. Of course, people are at liberty to take other extensions, but it will be in their interest. It will pretty much be dependent on the sort of package that we put

together for them. It's on the unique selling proposition that we'll craft with BRS.

ROCIO DE LA FUENTE: Thank you. Zerafinas, if you need a follow-up on that question, please, could you send it through the chat? I'm sure Gitau would be able to answer that through the Zoom chat. Thank you very much for your presentation.

Now it's time to move to our next speaker. I would like to introduce Irina Danelia. She's going to talk about new legislation and how it affects registry, registrar, and registrants. Irina, thank you. The floor is yours.

IRINA DANELIA: Thank you, Rocio. Good afternoon, everyone. Nice to be here. I had no topic to speak for a while and I'm really happy to have interesting news to share with you. September 1st, in my country, it's Day of Knowledge, and in many countries it's the date when kids go to school, and it's considered like a day when something really new starts. And this is our case. We really have new legislation requirements, which will significantly change the domain name industry in the country. All this happens in a year when we, as coordination centers, are celebrating our 25th anniversary. But instead of having a party and enjoying celebration, we are working hard to implement this new stuff.

What happened? The federal law was signed on 29 December of 2025, New Year gift, amazingly, which in general brings three new major novellas. First, it requires mandatory identification with the governmental service, which is called Unified Identification and Authentication System to register a domain name. This is not a completely new thing for people because this service is already used to identify customers for banking services, for some commercial services. It's also used to provide all the governmental services. It has also been introduced as identification mechanism for hosting services. But what is unique in the domain name case is that this is the only way to register the domain name. There are no other methods to identify the registrant mentioned in the law.

Second novella, the Coordination Center for .ru/.рф, as well as RosNIIROS, which is ccTLD manager for .su TLD, are appointed to act as registrars for the governmental organizations. And governmental organizations include state bodies, state and municipal unitary enterprises and institutions, as well as state-owned companies, publicly-owned companies. This is a completely new function for our organization, which we have never around before.

The third novella is that the domain name registration terms and conditions registrar accreditation rules become governmental acts. This affects registries, registrars, registrants. For each of these topics, I could give an hour of presentation. Here, it will be only a very brief overview of what the challenges which are coming.

This mandatory identification via USIA is required not only to register a new domain, but also to renew to transfer the domain name. It is supposed to work quite smoothly for new registration, because when new customer comes, when logging into registrar, he will be suggested to login via this system and to give his consent that his identification data are transferred from the governmental system to registrar.

That's okay. But what about renewals? The concern here is the quality of the registration data. And if the set of data which comes from governmental system does not match the data that are already in registrar database, then what should registrar do and how he can know that the guy who logs in is the same who is in his system already?

Just one case to illustrate it. Young lady owns a small business. She sells clothes for kids. Six years ago, she asked a webmaster to set up a web shop for her. And he registered domain name, installed web shop. A domain name, by the way, is registered for the name of that webmaster. Renewals are paid from the credit card of this young lady. Everything works smoothly until after September 1st, she will be suggested to login via USIA to confirm her renewal. How would she do it? Their webmaster has gone to Serbia. It's not available anymore.

That's the first issue. We're trying to make all the registrants aware of the issue and strongly suggest them to check their registration data and to make sure that they have right set of data in the

registrar's database. And if there are any corrections or adjustments needed, we suggest they do it right now or it will be too late then.

On the registrar's side. First, they are dealing with this requirement of identification. But secondly, to ensure this process, they need to connect their system to this governmental database. And since there are personal data transferred, there are quite strong requirements to ensure the secure channel between registrar and governmental system, which means it takes time and it takes money to purchase and to install necessary certified equipment and software to get approval for this interconnection.

In addition to that, as I mentioned, the accreditation rules become a governmental act. It's not accreditation anymore because accreditation already has another meaning in the state language, in the language of state documents. So it's inclusion in the newly formed list of domain name registrars. And again, that's fine for a new registrar because the procedure is described step by step. There is quite long enough timeframe, up to 90 calendar days and even more.

But what to do with the existing one? Until August 31st, there is accreditation that they had before. September 1st, the list is empty. And there is no transition period described by governmental acts at the moment. We internally discussed how we would arrange this transition to make it smooth. Hopefully we will manage to make it work without significant losses.

On the registry side. First, they have got a completely new line of business like serving registrants, which means we need information system, internal procedures, tariffs, stuff, connect our internal system to this governmental database. I think we will now fill ourselves very well in the shoes of the registrar. Though we're always trying to be connected and we have many employees who used to work registrar, but now we are exactly in the same boat with our registrars.

Then new set of policy documents. Though it was preliminary agreement that there will be not significant changes in the scope of the document, when terms and conditions become a governmental act, there are certain requirements on the layout of the document, on the terminology, and so on and so on. There are changes at least in format. And we were lucky to be involved in the process to develop this document from the beginning. We were able to submit our versions which were taken into consideration by the ministry, which is responsible for the entire law.

But the biggest challenge is the time pressure. Because even having started in January, we contacted the ministry and asked, "Well, when do we start?" They said, "Well, maybe end of February." In a week, they called back and said, "Listen, we have made calculation. We need first draft in a week. Are you able to submit it?" "Okay, we do." Then, "We need to do these changes. Are you able to make them in two days?" "Yes, we can." And further, further the documents move along the process, the timeframe gets shorter

and shorter. “Listen, we have this question and we need an answer in an hour.” Okay. That’s quite unique experience.

This is my last slide and it just demonstrates how the hierarchy of the policy documents changed. On the left side is the list of most of the documents we had before. Not all of them are included but at least the most important ones.

And on the right side, there is the new structure. The federal law, the three decree of government, the ministry act, and there are documents still at the registry level. Again, the main challenge is timeframe. Because the first decree is approved but the second and the third, which are rules of formation of this registrar list and domain name registration terms and conditions which were scheduled by June 1st. And I thought I would be able to tell you that it was approved and what is there. They are not published yet so we cannot move further with the documents below and finalize the procedures and many other things.

However, we’ve learned a lot. We learned how the governmental bureaucratic machine works, valuing how to be a registrar. And I hope we will manage and survive.

ROCIO DE LA FUENTE Thank you, Irina. Are there any questions? I see Pablo and Bruce. We have time for these two questions, and then we will try to have more comments in the end of the session. Pablo, go ahead.

PABLO RODRIGUEZ: Thank you, Rocio, and thank you, Irina, for a great presentation. Perhaps you talked about this already and I missed it, but I like very much the example you gave of the young lady that contract someone to develop the website, it was paid with a credit card, but the name doesn't appear there. What would she have to do? Would she send like a letter, put this in writing, notarized by lawyers, something like that to get it done?

IRINA DANELIA: At this moment, this is on registrar's side, and each of them develops their own procedures. Until September 1st, there is no any special regulation on this. If she will be able to convince registrar that she is not trying to steal this domain, the registrar will hopefully assist her to update the registration date. The challenge is that she has to know about it.

PABLO RODRIGUEZ: Thank you so much.

ROCIO DE LA FUENTE: Thank you. I think Bruce had a question.

BRUCE TONKIN: Thanks, Irina, for the presentation. I'm curious, what sort of driving that level of government regulation? Was there a large amount of abuse going on in .ru that drove that? What's the driver for those very specific rules?

IRINA DANELIA

Well, the initiative to let registrars use this governmental base came actually from us and from registrars five probably years ago we started this negotiation and how we can ensure that registrars are permitted to get access to this database. But we never meant it to be the only method. We meant it to be like additional method, which is really good to have verified source of data. Why it was limited to only one method? I can't comment.

With regard the state body's domain name, this is the attempt to ensure they are secure and that state organizations will not lose their domain names because of different factors, including the effect that they might just forget to renew it. There are minor differences in the life cycle for this specific group of domain names, like extended redemption grace period, for example, and mandatory registry lock.

ROCIO DE LA FUENTE

Okay. Thank you very much for the questions and the discussion. Now it's time to move on with our next presenter. Let me introduce you Fatma Demirel from .tr. She's going to talk about a new abuse mitigation mechanism in the .tr ccTLD. The floor is yours. Thank you.

FATMA DEMIREL

Thank you. This is Fatma Demirel from Turkiye. We are working under a governmental organization which is Information and

Communication Technologies Authority, which is related to the Ministry of Transport and Infrastructure. Before moving to abuse prevention mechanism that we are conducting, I want to mention about who we are and what we are doing. Next slide.

In Turkey, we are managing .tr domain names under our agency. And recently, we have an active 1.3 billion domain names in our systems. And also, we implemented the .tr [flat] name period, sunrise period recently. We have over 200,000 domain [flat] names format in our systems. And we launched TRABiS three years ago, and until now we have approximately one million domain names need to register after TRABiS's launch. And also, we have a well-structured dispute resolution mechanism in our systems and we have sold approximately 100 disputes in our system.

When we look at the evolution of .tr, it was managed by a university in our country, and then we did an agreement between university and our agency. We started to redelegate .tr from university to our institution. In the scope of that, in 2019, the IANA record delegation changed to our institution. And then we did necessary preparation. In 2022, TRABiS became operational, actually. With TRABiS, we had some nearly application in our systems. Now, we are doing it in a legal framework, actually. Also, we did lots of works to modern and to renew our technical systems within the scope of our institution.

Now it's time to move to today's topic. I will talk about our abuse mitigation mechanism in our country. But it's not a Tech Day

session, because of that, I will talk in terms of the policy perspective and I will summarize how are the policies published.

ROCIO DE LA FUENTE: Sorry to interrupt. Could you please slow down a little bit for interpretation purposes? Thank you.

FATMA DEMIREL: Okay. Let's move. We have a legal framework in our country, which is Electronic Communication Law. There is an Article 60 and it covers that we have to protect public institution, organization, and a real legal person against cyber attacks. This is a general article and we are doing all abuse operation under that article.

I want to summarize our abuse mechanism in three parts. We are detecting the abusive domain names before registered. And in the second category, we are detecting and analyzing domain names just after registered. Because in daily, we registered 1000 domain names in our country. And in each day, we are scanning these domain names with the help of our AI tool, and we are labeling some of them are abusive or not. The third category is about routine and daily scanning. We are scanning all domain names in a period and we are detecting the abusive activity. In that manner, we are using a machine learning model, we call this AZAD. And also, we are using another application, which is for just incident management, we call it KULE. Let's move on.

When we look at the operational flow, we are actively taking incidents from our stakeholders which are registrars and end users. And also, we are doing proactive works with our AI tool and we are collecting incidents. After collecting incidents, we are evaluating and we make a decision to suspend or cancel a domain name.

We will look at our system volume as far as—until now, we have more than 13,000 complaints in our systems. We evaluate them and the 5000 verified abuse cases we detected and we delayed or we suspended domain names. Then we'll look at the extension, mostly they were com, net, and org.

When we look at the categories, as you predicted, most of them are phishing and malware attacks. When we look at the keywords, we are seeing that opportunity, campaign, discount, basket, at your door, online and trust were mostly used for abusive activities.

As I mentioned, we were trying to solve it in three categories. This is our first category. We are trying to detect a domain name before registration because we have a restricted names policy. In this policy, we have some keywords like bank, finance, ministry. And if a domain name includes these keywords, we are doing a secondary review and document verification before assigning and before giving these domain names to our registrant. As a result of this policy, there is no phishing attack about banking because bank is a restricted word in our system.

We will look at the perspective from market evaluation and regulatory response. Before TRABiS, com, net, and org extension

were assigned with documents. After TRABiS, we are allocating them without documentation. It has many advantages and also some risks. The volume of domain names increases, but the abuse rates and abuse volume also increase. Because of that, we need a well-structured policy.

In that part, we started to do a bottom-up policy development process. In that manner, as I said, there was a general rule in our systems and we need some secondary legislation to do that. Because of that, we started to write it. But it is a bottom-up policy development process. We gave some feedbacks from our stakeholders, and also we had an operational experience from our registrant, and also we have a governmental perspective to protect our citizens, actually. When we collect three of them, we come to bottom-up policy development process.

As I said, there was not many domains in the systems, and after TRABiS the volume of the domain names increased. As Irina explained also, we are talking about the identity verification in the .tr. And maybe I can present it for the coming events in that sense.

As I said, we accumulated operational experiences from our registrant in those three years experiences. And then we have communiqué and we open this communiqué for the public comment, and over 200 pages we collected feedbacks and we evaluate them. Also, as I said, we have a governmental perspective to protect our citizens and collecting them, we did bottom-up policy development process.

I missed to say, we were also working with our third cyber emergency response team. But now, as I said, we want to work ourselves in our TRABiS systems and we are doing some changes in our legal texts. We are doing secondary legislation and we are planning to do some workshop with our registrar. And finally, we will ensure the final implementation will align with real-world experiences.

I think some of them also have some problem to define abuse. We investigated and did many research to define what is abuse. When we look at ICANN's and the other text, we detected that there are just categories, malware, phishing, botnet and pharming, and spam, but there was no concrete definition. And we did a definition in it. Maybe it can be beneficial for your country. We said abuse as an abuse of a domain name systems refer to activities that involves the intentional or malicious use of domain names and DNS infrastructure associated with domain names for the purpose of harming Internet users which targets availability, integrity, or confidentiality of information systems. We define it like that.

As a summary, as I said before, after TRABiS's launch, we had great operational experiences about abuse, and then we collect some feedbacks from our stakeholders and registrars. And now we are recently working on our legal texts. It did not publish yet. We will publish it soon. And we are aiming to design a well-structured legal text to define our registrar roles and obligations and their duties in that text, actually.

That's all. It's the end my presentation. If you have any question, I can answer it. I know we are all trying to find solutions to same problems. Thank you.

ROCIO DE LA FUENTE: So we have some minutes for questions and comments. Yes. I see a hand there and another there. So can you please introduce you and your ccTLD?

DAVID: It's David here from cira.ca. Thanks for the presentation. I was wondering if you could elaborate a little bit on your workflow for the secondary review process regarding those AI-generated reports? I guess specifically, I'm wondering, how do you balance human in the loop validation with the volume and scale of the automated detection coming in?

FATMA DEMIREL: As far as I understand, you're asking about our AI tools, how it's working, and how it's doing the detection and labeling.

DAVID: Yes. So if you've got all these reports coming in from the automated tool, like how do you review those reports at a human level to make sure there are no false positives?

FATMA DEMIREL: Okay. As I said before, we registered 1000 approximately domains in each day, then we have a threshold point in our systems in our AI model. And if a domain name is under this threshold, we labeled it as abusive. Then our operator doing a manual process, as you know, we use total, WHOIS data or source code, they are investigating these tools to be sure that there is an abusive activity in that. If there is an evidence, we labeled it as an abusive activity and we decide to suspend or delete this domain name.

DAVID: Okay. Thank you.

FATMA DEMIREL: You're welcome.

NICK WENBAN-SMITH: Thanks, Fatma, for the great presentation. It's Nick Wenban-Smith, .uk. We've spent many times looking at abuse and the definition of abuse, and what should be included, what should not be included. I was really interested in your formulation of the definition of abuse because it's incredibly wide. And then if it's useful to go back a couple of slides?

FATMA DEMIREL: Maybe you like it.

NICK WENBAN-SMITH Well, I was going to ask you, would, for example, Facebook, which steals users' personal data intentionally, cause causes harm. It does use the confidentiality of information systems. The definition is very broad, right? So, it could include platforms, it could include things which are harmful but lawful in the normal course.

FATMA DEMIREL But the text is under the domain names and it is restricted with the DNS infrastructure. Because if we got it broader, that can be about content issue, but we are not responsible for the contents, just we are looking at DNS infrastructure and we are detecting this as an abuse of activity under the technical capacity. Because phishing, pharming, malware, and all of them are a bit related with the DNS infrastructure, also spam.

NICK WENBAN-SMITH So, although the definition is formulated extremely broad terms, in fact, you're really concerned with the technical abuses of the DNS infrastructure.

FATMA DEMIREL Yes. We are looking at the side of the technical parts. Another, laws in our country and looking at them to the content part.

NICK WENBAN-SMITH Fine. Okay. Because obviously we as registries find it difficult to become the policemen of the whole Internet and all content issues, and that's really hard.

FATMA DEMIREL We have other roles in our country, and they are handling other things.

NICK WENBAN-SMITH Thank you. Thank you very much.

FATMA DEMIREL Welcome.

ROCIO DE LA FUENTE Thank you very much for the very interesting discussion. In the interest of time, we have to move on with our next presenter. I want to let everyone know that he's going to speak in French so please have your headset ready. Idrissa is going to talk about intelligent safeguards against DNS abuse at .sn. Thank you. Let's give everyone a minute to get their headsets. The floor is yours. Thank you.

IDRISSA SARR Thank you very much, Rocio, for introducing me. I am going to share with you the practices that we have implemented at the .sn. I hope that you all have your headsets, that you are ready.

Let's have a look at how we managed to create another tool, a new tool, in order to control DNS abuse, and that's without changing our policy or our rules. Just a quick reminder, the .sn is, so to speak, a small registry. We have about 12,000 domain names. Our customers are present throughout the world. We have registrars, we have 67 of them, or almost, and most of these of those registrars are overseas.

So, what does this mean? Well, it means that people can register in .sn wherever they are in the world and they can also use artificial intelligence, which means that there are more DNS abuse cases or at least attempts to take over a domain name. But what is worse is that we noticed that the number of attacks or attempts made it through the filters. So what does this mean? This means that the filter is not updated or upgraded to deal with those attempts.

So, what is the goal? The goal is to figure out how to alert AI. Could we possibly build a flexible tool, a flexible system, in order to reduce the consequences and DNS abuse without having to change the rules? If we change the rules, let's hope that we can do so in a minimal manner. Because changing the rules is not easy, especially when you're dealing with a global situation.

So, just to give you a little bit of an idea of how the system worked and to give you an idea of what we implemented in terms of changes, I'll give you the traditional model that we used. That's what you have on the screen. We had a number of reserved terms or forbidden terms. Those terms were considered as the terms we

had to protect. Those were also terms that we considered as terms that should not be accepted because of our social and cultural context, and also because of the public services, government services. So, first, you have reserved terms and you have forbidden terms.

Based on that, we also had all of the domain names. Of course, we have grammatical rules or syntaxic rules that will need to be considered, so that's how we managed abuse. And then we had the control layer with three types of outcomes or decisions.

First one was to accept the domain name, so that it's in conformity with our rules, or to be rejected because there was an issue, there was a violation of our rules. And the third option was to have those terms being verified some more. So the documents that need to be provided or explanations that are going to enable us to assess the situation. And once we have this, we'll be able to accept this new domain name or refuse this domain name. That's how our system works.

When AI arrived and we had the language, which is our language [well-off]. And some people use some reserved terms or were able to circumvent our control system. Six months ago, we noted that someone was able to create more than 200 domain names that were forbidden in our system. They used AI to register those names, and it was time when we realized that that we reviewed the system. And this is the schematic we have on the screen. It seems quite complicated, but we are trying to show how AI is used in our control

system. You have on the left the reserved terms that we saw, and the domain names that are registered, and all the syntax rules to be observed.

We looked at the history of the complaints that we'd receive earlier. Of course, we noted what was detected regarding the use of those domain names. So we do have one of our local languages which is our official language, and everything is integrated in our analysis system so that we can verify those domain names when they are created.

This is a two-layer system. When there is the creation of the domain, the name is verified, and we are looking at all the entries that we received. That domain name, isn't it identical to a forbidden term? Because people are using [well-off] terms close to the reserved terms so that they go and circumvent and go around this. Now we're able to detect that and prevent that. With the IDNs, we noted that people are using accents or special characters to circumvent our control.

So that's the control at the registration level that we have. At this level, even if the domain name goes through, we have a verification that is being done for later on. Certain domain names are noted or are tagged because we know that those domain names are acceptable now, but later on they could be used in another way. So registration of that domain name, but those tagged domain names are verified regularly. But from time to time, we do a post registration control. And all the domain names that are being

created since the beginning of .sn, we choose at random some domain names and we do verify the cost of associated services, associated domain. We're looking at the web pages, we're looking through scrapping. We're able to go back to web pages and we're looking at the content isn't corresponding to what was declared by the owner of the domain.

So sometimes we have to block the server, we ask for extra information, or there is a suspension when we are certain that there was an issue with that domain name. That's how we went from the classic model to our two-level system with verification when registration of a domain name and continuous verification using AI and using manual verifications.

So, how does it work now? Regarding the registry, we do have a control board that enables us to see all the domain names that were created in the last 72 hours, for instance. And we do verify the domain names that need to be verified some more because they weren't caught during registration. But there's no automatic rejection. We do communicate with the owners to see what the problem can be. And sometimes we do have to ask many additional information. So we're not doing it looking at all the domain names but only looking at the suspect domain names.

Regarding the registrars, what is going to be different? When you create a domain name, the user or the owner can look at all the domain names and the variants with our local language. And with IDNs, all the possibilities are presented. That's how IDs can be

taken over, and we're asking the user or the owner to block them, or to register them all, or to do the necessary follow-up. So the client, when you register a domain name, will have a better knowledge of the possible abuse on those domain names. This is something new. This is something that we offer now.

I would like to let you know that we still have our usual way of working. We're using AI, as I explained, but we also work manually, as usual as before, especially when there is blocking of domain name, we do ask questions. And we have a team made of humans that are asking questions and doing their oversight. We can update the reserved names. They were not automatically updated. Now every time we have a domain name, we are looking at all the domain names that need to be checked or that can be blocked because they have those forbidden terms. And our database is being updated that way. And we do still have a strong transparency. Every time there is a suspension, every time you cannot use a domain name, you'll be told what happened and why you're not respecting the charter, so that you understand why the decision was taken.

So, in sum, that's what I wanted to share with you, an update of our tools and our use of AI without changing the way we worked previously in full transparency so that our services are continuous and working well. Thank you very much.

ROCIO DE LA FUENTE Are there any questions, comments? Please.

UNIDENTIFIED PARTICIPANT Thank you very much for this most interesting presentation. Now, in terms of false positives, do you have a process to manage the claims, or at what frequency do you have these false positives? My apologies for the French.

IDRISSA SARR It was perfect. Yes, in terms of domain names, when they are suspended, the customer can lodge a claim, so there's a procedure. At times we actually meet the customer to explain why the name was blocked. Sometimes the customer does not contact us directly, they go through the registrar. So we speak with the registrars and they inform the client. To give you a recent example, the customer didn't come to us, they came to the registrar, and so we gave the registrar all of the information needed and the why. Why this user, why this name holder was blocked.

UNIDENTIFIED PARTICIPANT Thank you very much.

IDRISSA SARR You're most welcome.

ROCIO DE LA FUENTE One minute so please be brief. Go ahead.

UNIDENTIFIED PARTICIPANT Thank you very much. I will speak very fast so nobody can translate, but thank you for the presentation. I just have a quick question on whether or not you had any disputes? Because some name holders perhaps were not questioning but threatening or questioned your decision.

IDRISSA SARR Yes, we did have a very specific case with our national newspaper. When it was detected, we blocked the domain name. They came back with a lot of documents. What happened is that we exchanged with them and we gave them all of the information related to charter that they had violated. And based on that they said, "Okay, we were at fault." On the other elements, they didn't agree. But when they were proven that they were in violation, basically, there is a sanction. They accepted and they pulled back, they stopped the dispute.

ROCIO DE LA FUENTE Thank you very much. Please join me thanking our speakers today. Before we close, I would like to invite everyone to participate in the post-meeting satisfaction survey, as well as the Mentimeter poll that I think will appear on the screen now. Lastly, I just want to mention that this discussion provides an interesting transition to our next session which is going to be about ccTLD and registrars

tackling DNS abuse. So, thank you very much, everyone, and see you in a bit.

ALEJANDRA REYNOSO: Before you leave the room, let me make a quick announcement. This is Alejandra Reynoso. Hello. As you may remember, we asked the community for some photos of Bart. Right now at the coffee break, we will have coffee and cake here in the room, and we will have a slideshow with all the photos that you sent. So, please stay in the room and join us. Thank you.

[END OF TRANSCRIPTION]