ICANN86 Seville | PF – NextGen@ICANN Presentations (2 of 2)
Wednesday, June 10, 2026 – 11:45 to 13:15 CEST

FERNANDA IUNES: Hello, everyone. Welcome again to our second NextGen at ICANN Presentations. We are really excited to hear these next speakers today, but before we begin, I'll hand it over to Siranush for the script.

SIRANUSH VARDANYAN: Thank you, Fernanda. Hello, and welcome to the NextGen Presentation Day 2. My name is Siranush Vardanyan, and I am a participation manager for this session. Please note that this session is being recorded and is governed by the ICANN Community Participant Code of Conduct, ICANN Expected Standards of Behavior, and the ICANN Community Anti-Harassment Policy. Please observe the following guidelines to participate in this session. I have also posted them in the chat for your reference.

During this session, questions will only be read aloud if submitted within the Q&A pod. 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 in Zoom. On-site participants will use a physical microphone to speak.

Note: The following is the output resulting from transcribing an audio file into a word/text document. Although the transcription is largely accurate, in some cases may be incomplete or inaccurate due to inaudible passages and grammatical corrections. It is posted as an aid to the original audio file but should not be treated as an authoritative record.

Only questions posted in Q&A pod will be read aloud during the session, as time permits, and when directed by the chair of the session. Please state your name for the record, the language you will speak, if speaking a language other than English, and speak clearly at a moderate pace. I will now hand back to Fernanda.

FERNANDA IUNES: Thank you so much, Siranush. All right, and without further ado, so that we can have as much time as we can for questions, let's begin. Our first speaker is Haoua Annour Nassir. Haoua, the floor is yours.

HAOUA ANNOUR NASSIR: Hello, everyone. My name is Haoua Annour Nassir, and I am from Chad. I am currently a student in France studying development, sociology, labor, and association expertise. So today I am going to present to you a very true reality that is happening in Chad, something that many people are facing in Chad.

When I have been selected to attend ICANN program, I called one of my colleagues, and I told him that I'm going to represent Chad in Spain. And he told me, "What can you present like a reality of Chadian to people who don't know how Chadian people are suffering from the internet?" I'm not saying that we are victims, but we are facing so many digital realities in Chad. So today I'm going to talk about the digital divide in Chad, internet governance, and why digital inclusion is important for young people and communities.

So before I start, I would like to ask a quick question. How many of you used the internet today before coming here? Probably most, I think. Yes, most of you. So now imagine living in a country where connecting to the internet is difficult, expensive, and sometimes impossible. This is the reality for many Chadian people.

So first of all, I would like to define the digital divide. I know that this topic has been discussed for many years for so long time during ICANN program. But this is new for Chadian people. Let's talk about it. So the digital divide refers to inequalities in access to digital technologies and the internet. It's not only about having a computer or a phone. It is about having a reliable connection, affordable internet, and the skills needed to use digital tools effectively. This is what led me to ask a question. How do Internet governance and infrastructure development contribute to the digital divide in Chad between the urban and rural areas?

This is in N'Djamena, the capital city, so internet access is generally easier, network coverage is better, but not best. Mobile data is more available, and people have more opportunities to use digital services. When I talk about in N'Djamena, I'm not saying that internet access is excellent. In fact, many users in the capital still experience slow speeds, network interruptions, and high data costs. Compared to the major cities in Europe, North America, or even some African countries, internet access in N'Djamena remains limited. However, N'Djamena generally has better connectivity

and more digital opportunities than many rural areas in Chad. This comparison I'm making is therefore within the Chadian context.

The digital divide exists not only between Chad and developed countries, but also between the capital and city and more remote regions such as Fianga. This is Fianga. It is situated in South Africa, South Chad, and it represents a different reality. Many people in this village face weak or unstable network coverage, limited electricity, and difficulties to connect to the internet. These limitations affect everyday life. Students may struggle to access educational resources, and local businesses may have fewer opportunities to use digital tools. This example shows that where you live can strongly influence your digital opportunities. The reality of internet access in Chad.

To better understand the digital divide in Chad, let's look at some key figures. According to the 2025 digital report, Chad has a population of approximately 20.7 million people. What is particularly interesting is that Chad has a very young population. with a median age of 15 years old. However, around 75% of the population lives in the rural areas. This is important because rural regions often have less developed digital infrastructure, making internet access more difficult. What I find particularly striking is the gap between mobile connectivity and actual internet use. There are around 14 million mobile connections in the country, representing nearly 70% of the population. This shows that many

people have access to a phone, but not necessarily to affordable and reliable internet services.

So these are the two main telecommunications operators in Chad, Airtel Africa and Move Afrika. So they play a crucial role in providing connectivity throughout the country. However, users often experience slow internet speeds, network interruptions, and unstable connections. Coverage is also uneven, with urban areas receiving better service than many rural areas. These challenges contribute to the persistence of the digital divide.

Another major issue is the affordability. Internet data can cost between 1,500 and 2,000 FCFA per gigabyte. For many households and students, this represents a significant expense. When Internet becomes too expensive, people are forced to limit their usage, rely on public Wi-Fi, or simply go without access. So the digital divide is not only technical, it is also economic.

After discussing the challenges, I would like to talk about the project to reduce this digital divide. Reducing the digital divide requires collaboration between local communities, technical organizations such as ICANN, telecommunications operators, and the government in Chad. One idea that I propose, and I propose to my community, is the creation of community of DNS hubs in rural areas such as Fianga. These small local hubs could improve access to online content by reducing latency and making internet connections more efficient. Another proposal is the development of local internet governance laboratories in universities and

schools. These centers could train students in DNS management, internet governance, and the digital infrastructure, helping to build local technical expertise.

As an ICANN NextGen participant, I see ICANN not only as a global organization but also as a potential partner for local initiatives in Chad. When I come back to France, I would like to organize a debriefing online to share my experiences with my colleagues who are in Chad, because I am also involved in an association which is called Youth Association for Education and Environmental Protection.

So, in this association, we have part of education. In the part of education, we will talk about the technologies because most young people in Chad are interested in digital technologies, but they don't have access to the internet, so they need to have training. And I hope that ICANN can support workshops and awareness activities organized with local associations like mine, universities, and youth groups. Throughout these partnerships, young people could learn more about the DNS, internet governance, and how the internet actually works in Chad. Because they don't have this opportunity to know more about the digital divide.

To conclude, the digital divide in Chad is both a technological and a social issue. Significant differences may remain between urban and rural areas regarding access, affordability, and opportunities. So to reduce these inequalities, we said it will require investment in infrastructure, stronger education, and collaboration between

the governments. So that's what we are going to do. And thank you for your attention. And if you have any questions or advice, you can give it to me. You are welcome. Thank you.

FERNANDA IUNES Thank you, Haoua. Wonderful presentation. Any questions for Haoua? Peter, go ahead, please.

PETER JIA WEI CUI Hello, and I'm Peter. I'm from Taiwan. I'm a TWNIC Academy Fellow, and thanks for sharing. It is actually a very wonderful sharing and observation about Chad. My question will be, because recently there's a lot of discussions on, for example, Starlink and all these kinds of satellite-based internet access platforms, I wonder if these kinds of new platforms can help improve the internet access in Chad, or if there are some challenges in Chad as well.

HAOUA ANNOUR NASSIR Now we have Starlink in Chad, but it's very expensive for many people. It's very, very, very expensive for many households and for students. Even at the university, we don't have access to this opportunity. So, Starlink is only for rich people. Sorry for the word, but it's only for rich people, not for households or students who are living in poverty.

ALFREDO CALDERON: This is Alfredo. I'm a mentor for the NextGeners. My question for you is, have you explored, besides that idea of the community hubs, DNS Hubs, going outside of ICANN and exploring other organizations like Internet Society, if there's a chapter in Chad or nearby that you can seek out to help you. ICANN, through your Global Stakeholder Engagement Team in your region, can also help you to engage in all those activities that you want to do locally, and they are willing to support you with anything that you program with them. Okay?

HAOUA ANNOUR NASSIR: Thank you.

FERNANDA IUNES: Thank you. I'll hand it to Siranush for the online questions.

SIRANUSH VARDANYAN: There is a question from Emmanuel Oruko. "Very brilliant presentation. Have you considered partnering with Internet Society to establish community networks? This can support bridging the gap."

FERNANDA IUNES: Thank you. Yes, I think Alfredo also just talked about that as well. Thank you for the question.

ROBERTO GAETANO I posted that also in the chat in order to have the URL. There's a specific group that's a policy network on meaningful access, that, in the framework of the IGF, is addressing exactly those issues about internet accessibility in difficult areas and so on. And I would strongly recommend the presenter to join that group, to participate in that, because there's also a repository of best practices where there are examples of tools and ways to solve some of the issues related to bad connectivity, insufficient connectivity, and so on. Thank you.

JOHN CRANE John Crane, ICANN's Chief Technology Officer. Have you had the opportunity while here to meet with your ICANN colleagues from the region? If not, let me help you do that. We have a program that we're involved in called the Coalition for Digital Africa. We have trainers on the ground. We can help you meet other people through that coalition, not just ICANN, but many organizations that are interested in solving these problems on the continent. So if you need to meet people, many of them are here in Spain today, in Seville. So come talk to me afterwards if you need introductions.

HAOUA ANNOUR NASSIR Thank you, I'll come to you.

SEBASTIEN BACHOLLET Thank you very much for this presentation. I think I went three times to Chad for training purposes, and there are two At-Large

structures that are members of AFRALO, so it would be nice to get closer to them. You have, for instance, the Chadian chapter of the ISOC, the Internet Society. These are issues that have been raised for years. Things are being done by those partners. So I believe that just because you're a NextGen, you don't need to reinvent the wheel, you know. There are people in the field who are doing what you want to do. So get closer to them. And if you don't have their contact details, I can give them to you. But it's important not to be left alone by yourself. That is what ICANN does, and it can help you. There are also the At-Large structures that are members of AFRALO that can help you, too. Thank you.

ZEINAB MOHAMED

Hello, good evening. This is Zeinab Mohamed. I am a former ICANN NextGen and a member of ISOC, Sudan chapter. And thank you for the presentation. I just want to add to her that she can also get use of the NextGen alumni network. She can find resources, and she can seek help from the former NextGen members on the initiative she wants to work with. On the ground, there is a lot of effort that ISOC has been doing in partnering with the local organizations and other related organizations.

Like for example, in Sudan, there has been a project with an organization like UNICEF to engage more and deliver by accessing to the internet and therefore helping, for example, the students in education. So I guess there is a lot of platforms and people she can

reach for in order to help her in her mission. All the best. Thank you so much for the time.

HAOUA ANNOUR NASSIR Thank you so much, Zeinab.

FERNANDA IUNES All right. Thank you. Thank you so much. A wonderful presentation, again. And with that, we'll move on to our second presenter. Humay, please.

HÜMAY ZEHRA ÖZER Hello, everyone. My name is Humay Zehra Ozer. I am from Turkey. So I study Master's in Statistics at Switzerland University of Bern. And I will present my research, which is called Quantifying DNS Resilience, a Statistical Framework for Global Internet Infrastructure.

Before we start, let me explain our main focus briefly. Why are we doing this? Today, we usually look at DNS only after a problem happens. But we want to look at DNS as a critical global infrastructure. Our main focus is to use statistics to measure DNS stability and see hidden risks before they become real failures. So, let's start with how DNS works in our daily lives. DNS is like an invisible backbone of the Internet. It translates domain names into IP addresses, as you know. Users do not see it because it works quietly in the background.

On this slide, I want to show three important points. The first one is critical dependency. Today, all modern systems need DNS to work. But current tools are reactive. They only look at problems after they happen. The second one is strategic mission. ICANN works to keep the internet secure and stable, as we know. To do this, we must find hidden risks before a crash happens. And the third one is the research gap. Actually, my question is, can we use statistical models to predict future failure risks and build proactive resilience?

After talking about the risks, let's look at what happens in the real world when DNS fails. This slide shows the famous DNS outage. It shows that a single technical failure can create a massive global crisis. So this creates three big consequences. The first one is, of course, the system loss. Major platforms like Facebook, Instagram, YouTube become completely inaccessible. We cannot just watch the system; we must estimate the risks earlier. And the second one is economic impact. Outages cost billions of dollars. Monitoring tools can report the loss, but they cannot prevent the damage. And the last one is interconnectivity. Because the internet is connected everywhere, a small local error can become a global crisis very quickly.

To prevent this global crisis, we need to understand that DNS is not just a simple one step. It is a chain. DNS is a big ecosystem chain, as I said, and we focus on three main components here. The first one is root servers, the starting point for every resolution process. And the second one is TLD servers. They direct queries to specific

domains like .com or .org. And the recursive servers, they are like the librarians of the web because they find and catch the final answers. And if one link in this chain fails, the whole internet suffers. So we must measure the resonance of the whole chain, not just isolated servers.

Now that we saw the chain, how can we measure it like engineers? Complex systems need clear engineering pillars to stay stable. Our framework uses three main concepts. The first one is reliability. Actually, this is the most important one. The probability that a component works perfectly over time. We can calculate this using real statistical data that we got from the past. And the second one is fault tolerance. The system's power to continue working even during a local crash. And the last one is redundancy. Having backup server nodes and statistics can help us find the optimum number of backups that we need.

So, from these engineering concepts, we can use a specific and really special mathematical model for DNS redundancy. DNS is designed to avoid single points of failure. To calculate this, we can use K-out-of-N model. Let's look at the symbols of the slide. N is the total number of available server nodes, and K is the minimum number of active nodes we need to keep the system running. And R is the reliability of a single node. So the logic is really simple. This system stays alive as long as at least K out of N nodes are working correctly. This buffer protects the internet against traffic surges and, of course, outages.

Now let's see how this model looks when we spread it through the network. This slide shows our stochastic risk propagation model. Actually, stochastic means that the system has uncertainty and randomness. We cannot know the future perfectly, of course, but we can estimate the risk patterns. So predictive power refers to the ability to identify potential risk before they happen. As you can see on the red curve on the slide, a small local failure can spread and create a ripple effect across the network. This helps us identify critical weak points early and prevent small failures from becoming large-scale disruptions. And for the dynamic estimation, instead of just measuring uptime after a crisis, this model calculates a proactive resonance score before a crisis happens.

This brings us to the central change of my research, which you can see in this comparison table. First, the temporal focus changes. Current monitoring asks, what is happening right now? But our model asks, what could happen next? What will happen? Second, the operational nature shifts from reactive, the fixing errors, to predictive managing risk before it happens. And the third, the analytical method moves from just watching data telemetry to using statistical resonance estimation. And finally, the outcome goal shifts from basic uptime maintenance to resonance engineering.

So, why does this statistical shift matter for Internet governance and, of course, ICANN? This model is not just for engineers; it helps in three ways. For the policy support, it transforms complex system data into clear objective facts for ICANN regulations. And for the

SSR goals, it helps ICANN meet its security, stability, and resiliency goals by focusing on long-term engineering. And for the stakeholders, in ICANN's multi-stakeholder model, it creates a simple shared language for both technical operators and non-technical policy makers.

So now let's look at how we can build this framework using the tools and data ICANN already has. Our framework does not replace anything. It acts like analytical glue to connect them. On this slide, we focus on the data we can get from three major ICANN resources.

First RSSA data, we get critical performance and stability metrics from the root server system advisory committee. Second, DAAR data, we pull security data and malicious threat patterns from the Domain Abuse Activity Reporting System. Third, ITHI data, we collect ecosystem wellness indicators from the Identify Technologies Health Indicators Project. Currently, these groups and tools look at isolated sectors, so our statistical framework connects all this available data together to calculate just one unified Resilience Score for us.

After connecting these tools, who will benefit from these Resilience Scores? Of course, the whole Internet community benefits. Operators can use this data for better capacity planning during heavy traffic spikes. Security teams can find weak spots and potential failure zones before an attack happens. And policymakers can make better risk-based decisions for global Internet governance.

To conclude my presentation today, DNS is a critical part of the global digital world. As the internet grows, resilience becomes more important. My research shows that statistical modeling can move us from a reactive posture to a proactive posture. Our goal is to understand risk and support better decision-making. So I want to finish my presentation with this note. We cannot manage what we do not measure, and we cannot protect what we do not understand. Thank you so much for your time.

JOHN LEVINE: This is John Levine from the SSAC. This is an interesting talk, and I'm glad it's a topic you're thinking about. But I worry a little bit about what we call the light post problem, which is that you measure what's easy to measure. And I'm thinking, for example, that there's way more domains at Cloudflare than there are in 90% of the TLDs. And there's more stuff that routes through Akamai.

So I'm wondering to what extent you have attempted to, and your reference to Dyn was also a good example. So I'm wondering to what extent you're looking at these large non-TLD DNS providers as part of your risk model. And it happens that most of these companies actually have people here. I mean, I can introduce you to someone from Cloudflare if you want to talk to them.

HÜMAY ZEHRA ÖZER: Actually, first of all, I want to talk about the reliability theory that I want to use for this research. It's a really complex statistical thing,

and we can use it for, like, series system, parallel system, and also complex system that contain both of them. So if we can get data from different communities, we can give weights for each of them, and we can calculate these resonance scores, reliability scores for each of them, and connect them together. But, of course, we need data from the past and from the local or global crisis as well.

SAMWEL KARIUKI: My name is Samwel Kariuki, an ICANN86 fellow, for the record. My question would be, which kind of evolution metric are you trying to measure? Is it maybe accuracy? Is it precision? Could you kindly elaborate so that we are able to understand which evolution metric you are trying to measure in your research? I have an interest in this because I'm also doing research on the DNS attack and abuse.

HÜMAY ZEHRA ÖZER: So firstly, I want to talk about the reliability. Reliability is the probability that a system performs its intended function successfully over a specific period of time, and we can say a threshold time. And I want to also calculate the resilience for the system, and resilience is broader than reliability. It includes the ability to withstand distributions, adapt to changing conditions, and recover after failures as well. So these are the metrics that I want to calculate and find the probabilities.

JOHN CRANE

I promised I wouldn't ask you a question, but sorry, I'm going to. John Crane, Chief Technology Officer at ICANN. I like how you're thinking. I like your approach to statistically measure things. I will try and read your thesis when I get back from this. One of the questions I have for you, it is important to measure things, but it's also important to measure things that then become actionable and can change behaviors.

You talk a lot about things that ICANN can do, but it's important, I think, to understand how the operational side of this infrastructure works and the limits in ICANN's operational role. Now, of course, policy does have effect on how people implement things, but some of the data sets you're using, it's not 100% clear how they will relate to the resilience of the infrastructure, but that's a discussion about data sources and getting the right data sources.

And I wonder how you get this methodology, not necessarily the data, but the methodology, to those who operate the infrastructure. Yes, the Cloudflares, but also the ccTLD operators, the DNS businesses that are out there, because there are businesses that are about building this infrastructure. And I wonder if you've thought about how you take it to that next step.

HÜMAY ZEHRA ÖZE

Actually, this is my strategic roadmap. If I can find data from the past with ICANN communities. Firstly, I will focus on machine learning. Actually, if we want to focus on machine learning integration, firstly, we should focus on the algorithm behind this.

And for the algorithm, we need to understand the mathematical and statistical logic for it. I will start to understand and find a really good theory for every data. And we cannot give weight for every data equally. So we cannot say every data is independent from each other.

So maybe with Naive Bayes or any algorithm, we should select any algorithm. Or we should create an algorithm for DNS reliability. And after that, we can develop a dashboard, and it can be user-friendly, even the stakeholders, policymakers can understand this dashboard really good. And after that, I want to do empirical stress tests, and we can evaluate the infrastructure against simulated massive traffic anomalies, DNS attacks, and systematic routing issues to validate empirical limits for our model. So, everything depends on the mathematics.

JOHN CRANE I did notice there was a lot of mathematics in your thesis. So the real question then for me going forward, and we'll have lots of conversations about this, I'm sure, is how you make this actionable by the people that get that data. Giving somebody a resilience score is great. It's a good step. But the next question is, how do they decide where they want to be in those scoring parameters, and how do we help them get to where they decide their level of risk is, etc.? So I think there's a lot. I like what you're doing. I think it really is thought-provoking. So thank you.

HÜMAY ZEHRA ÖZER Thank you so much for your feedback. As I said before, we need to look at the crisis that happened until today, and after that, we can decide the threshold for it. And if we can just build a bar from green to red, I think that everyone can understand it. Thank you so much.

RYM BADRAN Hello, everyone. Thank you for having me. My name is Rym Badran. I'm Lebanese. We're currently based in Dublin. And I'm a law student pursuing the European Master's in Law, Data and AI at Dublin City University, but also University of Avignon and the University of Pisa as an Erasmus Mundus scholar. So I will be presenting my research on DNS abuse mitigation as internet governance, particularly through a comparative lens between Europe and the Middle East.

So first things first, what is DNS abuse? So the ICANN defines DNS abuse as long as it fits within these five broad categories. So first, we have malware, which is the distribution of malicious software, viruses, or spyware, and they are intended to disrupt systems or to gather sensitive information. We also have botnets, which are networks of compromised devices, which are often controlled via a malicious domain and they are commanded by an attacker to perform coordinated illegal activities.

We also have phishing, and I think we all fell for it at once. So this is the practice of tricking users to reveal sensitive information by

masking as a trustworthy entity. We also have pharming, which is redirecting users to fraudulent websites or services by posing as the DNS or even hijacking routing. And finally, we have spam, which is unsolicited communication, especially if it's used primarily to deliver mechanisms to spread, for example, malware, botnets, or phishing links.

That being said, my comparison is between Europe and the Middle East, and you would ask why so. First, it's a personal decision as someone from the Middle East living in Europe, but it's also because both of these regions have a lot in common, but also a lot of differences. So they make a compelling case for comparison in similarities, a huge diaspora, historical links, but also in differences. A lot.

So, first thing, the European Commission in 2022 conducted a very holistic study on the state of DNS abuse in the union. They managed to analyze 1.68 million abuse domain names across the global DNS ecosystem. And their main finding was that European country code domains, such as .eu, .es, are consistently among the lowest levels of DNS abuse globally.

Now, for them, they found also that the highest rate of abuse was mostly linked to newly introduced generic top-level domains. And the most common attacks were phishing, botnets, and malware. Now, I would have loved to say similar statistics for the MENA region, but unfortunately, we do not have a comprehensive study for the region, which shows an initial gap between both of these

regions, because the MENA has a huge problem on data transparency and measurement gap.

Now, secondly, we know that the EU and Europe more broadly are more regulation-driven. So the EU has a very robust cybersecurity framework backed by the NIS2 directive, but also complemented by secondary regulations, such as the GDPR for personal data, as well as the DSA, which is the Digital Services Act. In the MENA region, most of the frameworks remain state-centered, and they are implemented from a security-driven approach. So if we want to find the regulation, we would find them mostly in cybercrime laws or even telecom regulations.

And more importantly, in Europe, they have more cooperation. So if an attack happens in France or in other EU member states, then other members can come to help. There is the DNS for EU initiative, which, for example, received seed funding from the EU. This is, unfortunately, again, not the case for the MENA region. And here it's also important to highlight that it's very hard to treat these regions as homogeneous. There are differences between the countries. So, for example, Europe between Western and Eastern. But also in the MENA, for example, Gulf countries tend to have more resources, so they can act faster than countries in the Levant.

And my main point that I want to make on the differences is that DNS abuse in Europe tends to be commercially driven. So there is an attack to steal your sensitive information to gain money.

However, in the MENA region, a lot of the attacks tend to be politically motivated.

So what do I mean by politically motivated? We have on the slide here, for example, the Sea Turtle campaign, which was revealed in 2019, but it's believed that it has been going on since 2017. And this is a campaign based on cyber espionage and DNS hijacking, coordinated by a state-sponsored threat actor, aligned with Turkish strategic interests. So most of the analysts believe that it was state-sponsored by the Turkish government.

And basically, within this campaign, a lot of other governments in the region were attacked. First, it started with governments in the MENA region, and then it reached Sweden and the US. So they were attacking the porters of the ministries of foreign affairs, intelligence agencies, military branches, but also some minority groups. Most of them were Kurdish military and minority groups, as well as the websites and the domains of think tanks. But there's a recent research that was published in 2023, which is the year where everything fell down in the region.

And you can see, I don't know if it's so clear, but for example, the research shows that it's very high the likelihood of threats against government portals. They highlighted specific governments that are at further risk. But also more interestingly, even NGOs, diplomats, defense contractors, and media were at risk of phishing campaigns. So we do have a trend in the MENA region when some governments are attacking other governments, but also some

governments attacking the domains of independent media, activists, political parties' websites. So this is even more important when there's civil unrest or protests in a specific country.

So what is currently being done to tackle DNS abuse? And I think it's very timely to have this presentation and this policy forum, as we are also discussing the policy development process for DNS abuse. So there is this happening. We have industry collaboration to ensure that the infrastructure is resilient as much as possible. There are also contractual obligations, as we have seen, for example, when registries are accredited by ICANN, and, for example, if they receive evidence-based information that there's an attack, they should take prompt action to deal with it. And, for example, if they do not, you can also go to ICANN, and ICANN is monitoring this compliance through targeted auditing, as well as complaint-driven monitoring.

But I want to also mostly focus on this point on suspension. So what usually happens, let's say a domain is attacked. Okay, it's intercepted. And it's being investigated. So, usually the immediate response often tends to be suspension. Because this is the fastest and the easiest way to deal with DNS abuse. Now, suspension, if it happens in Europe and someone is trying to steal your money, it's definitely inconvenient. But let's consider that you are an activist in Sudan, and you lead an independent media, and the state kind of also targeted specifically an attack on your website, and your

website is suspended. Then this is not only inconvenient, but also an attack on your human rights.

So this is why suspension, especially because it remains the fastest and the most easily implemented strategy to deal with DNS abuse by registries, is very problematic. It can have a significant impact, for example, on the freedom of expression when independent media are targeted. Also, privacy, because usually, there are also data breaches related to that. Freedom of assembly, if this information is used to spread the word about a protest.

But I want to focus on two main human rights that are the right to equal treatment, because as we know, mitigation mechanisms should be available equally, but also to take into account what's happening within a specific context, and then also the access to remedies. So far, when a domain is suspended, there are very few appeal or remedy processes to deal with it.

Which leads me to say that it's very hard to imagine a one-size-fits-all model to deal with DNS abuse. And for that reason, I tried my best to have some suggestions that are very humble, I think.

So first of all, we all know that the multi-stakeholder model is under attack and under pressure across the world with the current political climate, but it remains as the most distinguishing point of ICANN. And we personally wouldn't know that some DNS abuse is particularly affecting some minority groups or specific governments if it wasn't for the multi-stakeholder and the fact that

they have a word on the table. So it's also important to ensure that civil society is represented, as well as the diversity of stakeholders.

The second suggestion relates to the human rights impact assessment. So, a human rights impact assessment reveals that whenever a policy is being drafted at ICANN, we should not only consider it from the policy priorities, technical feasibility, but also consider does it have any impact on our human rights. And this is a basic recommendation that was pushed by a lot of civil society organizations that are also represented at ICANN, particularly Article 19.

And third, it's also interesting to borrow some concepts that already exist in other bodies of law. So, for example, international human rights, which provides the principle of proportionality. So it's how you can balance between an attack and the fact that suspension might be needed, but does that over supersede your human rights of that specific entity?

And also because, as I mentioned earlier, most of the mechanisms remain related to suspension, how can we ensure that there are safeguards against over-blocking? Fourth, and more importantly, to ensure clear notice and appeal mechanisms, so how can affected domains ensure that every domain suspended can be appealed, what is the dispute mechanism? So far, it's very rare to have that. And fifth is strengthen transparency reporting. So far, I think it's only the domain.org that does a lot of transparency reporting. Other registries do not, well, to some extent, like to publish a lot of

information on how many domains were suspended, and also to categorize them.

And six is also the importance to conduct region-specific studies. So we know that before this policy development process, the major step was to have data in order to inform evidence-based policy. And if a lot of regions lack the data and the research, how can we ensure that they are represented in the policy? So it's also important to, besides capacity building, also fund research in those regions.

So this is everything from my end. Here's my email and my LinkedIn, and I'm also very happy to discuss. I hope it was as clear as possible. Thank you so much.

UNKNOWN SPEAKER: Hi, this is AB for the record. Thank you for the presentation. The topic is timely and interesting, and I believe we lack a lot of comparative studies in what's so-called Middle East and North Africa region. Just an advice for future interventions, you know, be a little bit sensitive when it comes to maps, to borders, to terminologies, the use of MENA, representation of Middle East, all these terminologies, especially in settings like this. Thank you.

HÜMAY ZEHRA ÖZER: Thank you so much, and I totally understand. I also wish if I didn't use MENA but SWANO, but also want to be in line with the terminology that's been consistently used, and I acknowledge also,

as I mentioned, that those regions are very politically motivated, and it's not homogeneous. So what I did, it really doesn't do justice to a lot of the communities, the languages, and the fact that minority groups who I tried my best to represent. And I also acknowledge that I might be coming and speaking from a position of privilege. So thank you for your comment.

CHARBEL CHBEIR

Hello, my name is Charbel Chbeir for the record. First of all, I loved your presentation. And this is a specific question for you because you're Lebanese and from the Middle East. It's a tricky question. It's about GDPR. So my question is, the right to be forgotten is one of the characteristics of GDPR. VS security logs, okay?

In Europe, GDPR places strict limits on retaining and processing personal identification, what we know as PII, compared to the Middle East, and restrictions for Whois data availability. Did your comparative analysts find that the Middle Eastern data protection regime allows registries more legal flexibility to retain analysts and share domain metrics for abuse mitigation than European registries?

HÜMAY ZEHRA ÖZER

So thank you, Charbel. And I think I might need also to circle back and to find the data. But it's also interesting because I made sure to mention the GDPR in my research to tie it to the broader framework of this research. And the fact that so far I think in

Lebanon we do have the personal data law of 2019. The right to be forgotten, even in Europe, is mostly mentioned, and it's supported by the CJEU case law, for example, in the Google cases.

And I think it's important to mention that the fact that the data transfer flows between the MENA and the EU could also impact the fact that in the EU, they are more strict on what they can retain, whereby in the region, we tend to be I would say also less, more flexible. So I would circle back definitely on your question to be more accurate.

But I think the MENA region is also pretty new to have those kind of discussions formally. So Lebanon and Tunisia are one of the first countries to have personal data laws. This is not the case in others. So the fact that we are more flexible could be the reason, because we don't have national laws very well formulated on that question. So I hope that I answered your question as accurately as possible, but I would definitely circle back on it.

FERNANDA IUNES Thank you so much. Great job, Humay. Okay, next to our next speaker, Ariba Aleem.

ARIBA ALEEM Hello, good afternoon, everyone. My name is Ariba Aleem, and I'm a student of International Affairs and History at the University of Bonn in Germany. So, today I'll speak on a topic of universal acceptance, a topic that I'm passionate about. It's about linguistic

inclusion and digital accessibility, or UA in Europe. So, this topic is not from a purely technical perspective. As some of my friends have already captured the details of it in the previous presentation yesterday.

However, I will try to argue that Europe's biggest challenge is no longer the standards, but the real challenge on ground is of adoption, coordination, and governance. So by the end of this presentation, I intend to show why Europe is unusually well-positioned to lead a multilingual internet agenda, and what are the steps that can be implemented to make that happen.

So let's just revise on the basic question of what is universal acceptance? So the principle is very simple. Every valid domain name and email address should work everywhere, regardless of language, script, or length. Now that means three things.

First, internationalized domain names such as Arabic, Chinese, Cyrillic, or Greek names should be accepted by websites and applications. Second, internationalized email addresses should be accepted by forms, identity systems, and mail services. And lastly, new and long TLDs should be treated as normal inputs, not edge cases.

So one might ask the question, why is this urgent? We now have about 1200 plus active gTLDs, and most systems still reject many of them. 60 plus ID and country code TLDs cover 37 languages and English only represents about 57% of online content, and that data

is also declining. UA is no longer a niche compatibility issue. It is a prerequisite for a multilingual and equal internet.

So in this slide, I will ask, since we are in Europe, we need to discuss why UAE matters specifically for Europe. So Europe has 24 official EU languages and a dozen regional and minority languages. For Europe, UA is not just a technical cleanup project. It touches digital sovereignty, cross-border public services, minority language inclusion, and the digital decade's language equality ambitions. If a citizen's valid address fails in a government form or an online service because it contains a diacritic or a non-Latin script, the internet is functionally less available to that user than to others.

So the core problem that is underlined is the adoption gap and not the technology gap. Because the standards already exist, internationalized domain names exist, internationalized email addresses exist. You can see the graph where email address internationalization-ready or EAI email servers have seen some progress over the last years. Yet many systems still reject valid inputs.

And why does this happen? First, organizations continue to rely on outdated validation rules. Secondly, many users never encounter the problem themselves, so it receives very little attention. Third, development teams often prioritize other projects. And finally, the people affected rarely report the issue. They simply leave. As a result, the exclusion remains largely invisible.

So this is where I request the audience to look at UA through the lens of change management. You will notice that there is a clear pattern that emerges. Most organizations are somewhere between awareness and urgency. Many decision-makers have heard of UA, but it is not viewed as a pressing or an urgent issue.

Developer training remains limited. Implementation efforts are fragmented, and there is little coordination across sectors. In other words, the challenge is not knowing what needs to be done. The challenge is creating the momentum necessary to make that happen. What is missing is a coordinated mandate and a roadmap that turns UA from an optional best practice into mainstream requirement.

The stakeholder map. Who needs to act? So in my view, no single stakeholder can solve this challenge alone. Governments and regulators can provide policy direction and procurement requirements. The private sector can modernize systems and adopt UA-ready practices. Academia and civil society can raise awareness campaigns and build skills among future developers. Meanwhile, registries, registrars, and infrastructure providers play a critical role in ensuring operational readiness. As per my study, the progress depends on all of these groups moving together hand-in-hand rather than acting independently.

Now, the EU Accessibility Act offers a useful analogy. It scales digital inclusion through five mechanisms. A clear obligation, a broad sectoral scope, a market-driven access incentive, standards-

based implementation, and a transition timeline. Universal Acceptance can take an inspiration from this and incorporate it in its adoption. The lesson is not that the UA should completely copy Accessibility Act policy exactly. Rather, it shows that Europe already knows how to drive large-scale digital change when inclusion becomes a policy priority.

So let's see what the data tells us about Europe's UA opportunity. Europe already has a very high IDN infrastructure support, with roughly 88% of European ccTLDs supporting IDNs. Yet IDNs remain only about 1.2% of global domain registrations, and one cited a 2024 ecommerce study found IDN email acceptance rates around 39%. Registries themselves also report low public awareness. To summarize in one sentence, the supply side is largely ready, but the demand side and the system readiness are not.

So this is where a methodology of change management becomes useful. Using Kotter's framework, we can think about UA adoption as a structured transformation process. Step by step, we can see how first creating urgency with the European UA Readiness Index is essential. Secondly, Build a coalition across the Commission, ICANN, EURID, National NICs and Civil Society. Third, define a clear vision, UA-ready public services by 2030. Then, communicating, removing barriers through procurement and training, and generating early wins with pilot portals, sustaining momentum through annual reporting and funding. And finally, anchoring UA into standards, skills and procurement culture.

From technical issue to a strategic inclusion strategy. So in my last slide, the message is quite simple. Universal Acceptance should not be viewed solely as a technical matter. It is a digital inclusion strategy. It is an enabler of a multilingual internet. And it is a governance challenge that requires coordination across different sectors.

And lastly, it is also an opportunity. Organizations that become UA-ready will be better positioned to serve increasingly diverse online communities. Europe demonstrated through the GDR that it can set global digital standards. With this thought, I leave you. The technology is ready. The question is, are we ready to make the internet work for everyone? Thank you.

XIANHONG HU

This is Xianhong from UNESCO. I'd like to really congratulate this excellent research. Actually, as you may have seen on the first day and yesterday, UNESCO and ICANN have jointly launched a policy brief on advancing Universal Acceptance worldwide. And what you have done exactly sounds music to us because that's what we expect to see happening in all continents.

So I really extend my invitation to collaborate. I'm totally onboard on that ecosystem-wide strategy, inclusion, multi-stakeholder implementation, collaboration at all levels, not only at the national but also at the regional and international level. UNESCO has been fully onboard with this.

I like that we can continue this collaboration. It's a very, very important start to translate our strategy into action. Particularly, I like to be informed, to be up on the five pilot countries in the European region, because we've been discussing about piloting some member state countries to have the UA adoption in the forthcoming months and years, to give an example for all the other countries. Let's hope that the UA will be eventually mainstream to all the countries. Thank you.

ARIBA ALEEM: Thank you very much. I also attended the session yesterday, and it was a very insightful session. on Universal Acceptance and giving insights on how there is still the profound value of UA in education, multilingualism, and economic growth, and can create opportunities for everyone. Thank you.

SIRANUSH VARDANYAN: There is a question. "Is there a link to where the policy brief on advancing UA worldwide can be accessed?" So maybe the person missed it. So if there is a link, just let me know. I will put it in the chat.

XIANHONG HU: Yes, we do. I will send you the link. This policy brief is currently an open-source publication on the UNESCO website. You can simply Google "UNESCO ICANN policy brief on advanced Universal Acceptance." It's open source, it's up to everybody. You can

translate to your local language for your network. We are also being translated to French and all the other UN official languages, plus Portuguese, plus Swahili, plus some indigenous languages, including Quechua. So I do hope that itself is a multilingual act to join forces on that. And also, I will put it on my LinkedIn and other social media accounts. Thank you again for your attention.

FERNANDA IUNES

Thank you very much again, Ariba. Great job. We have one more presenter here. If we have time at the end, we'll come back, and you can ask her, okay? And Hugo, please, last but not least, go ahead.

HUGO RAMIREZ

Hola. Buenos dias. My name is Hugo. I'm currently a PhD student, and I would like to give an easy talk before lunch and leave you to think about how we talk, specifically in internet governance communities. First of all, internet governance happens in the open. This is driven by policies, standards, and protocols that are published by ICANN, IETF, W3C, different bodies.

And these policies have a huge deliberation process. Processes that take years, two or three years, or more. People jump in, jump out of the conversation. We have different working group chairs. And my question for today is, well, I'm interested in this deliberation process, specifically in the conversation that this

generates. These ones are publicly archived through mailing lists, GitHub, the transcripts that the ICANN provides.

And my question for today is, how can we analyze what these conversations reveal about the deliberation process? First of all, the speed. The speed at which the community interacts. It can be at the beginning, the middle, or the end. If it's some trending topic that the community is really engaged in but suddenly fades away, or if certain agenda, specific timing, and it progresses as time goes on, or something happens, and you need a deadline to be met, and everyone gathers at the end of the conversation. But not that, but also the sentiment of replies between the participants. This is important. Because now that we have a broad community, we might be able to pinpoint whether we have geopolitical tensions in the conversations.

Ultimately, these patterns, the speed, and the sentiment, we can start to associate with which ones end up in publications of these policies. My study case for today is the IETF, 18 years of mailing list data. The IETF, the Internet Engineering Task Force, is an open and consensus-driven body that is more focused on building standards for the Internet. Anyone can submit a draft, and the heavy work happens in the mailing list. The drafts are revised through community feedback and feedback also from the working groups, and if there is consensus, this is published as an RFC. So today I will present to you how the IETF talks, how the deliberation process happens in the IETF.

First of all, what is a conversation in the IETF? For a conversation, I group all of the emails related to a specific draft and treat them as one conversation. From that, we got 11,000 conversations throughout the 18 years out of 2.5 million emails, and those 11,000 conversations correspond to 11,000 drafts the community has worked on. 6,000 of them resulted in publications of an RFC -- actually, it's 5,000 -- end up in drafts.

Let's talk about how the speed of the conversation goes. Here we have our share of conversations. As I talk, we have three types. Late, progressive, and early. This can happen in the interactions at the beginning, if everyone is really engaged in the progressive side, or if everyone jumps in at the last part of the conversation. The dashed parts are conversations that didn't end up in publication. My takeaway here is that late conversations are increasing and more likely to end up in publication. As you can see, in the early 2000s, the IETF used to engage in a progressive way.

As time progressed, the IETF moved towards having late conversations. But this is also a reflection on how complicated the policy development has worked. Because we're looking now at conversations of two or three years plus. And also, for example, in the early conversations, everything is practically non-published. We further observed that this is just because the drafts are not getting adopted by working groups. So it doesn't get enough interaction, and the conversation just ends.

How does the community respond to each other? Here, we compute the sentiment of replies of each of the emails, and we observe two big groups. We call them flat and dynamic. Dynamic, we have really positive or really negative responses in the conversation. In the RFCs, we have, "This policy is so good, we love it," or really bad interactions as "We hate it." We see the sentiment of this. So, dynamic conversations, we have really positive, really negative responses. In contrast, flat conversations just stay the same. They have the same sentiment of reply.

Here we have our share of conversations. Solid is publications and dashed are non-publications. What we see here is that the IETF moves toward more flat conversations. They are less having emotional responses in this deliberation process. And we also observe that the community is having more of this share as well of flat. And heavily penalizing dynamic as we observe that in the years of 2016 and 2023, most of the conversations end up in rejection. But these two graphs show us macro tendencies on how the IETF works, but we can also do an analysis on a regional perspective.

Given that we have geopolitical tensions around the globe, we wanted to see if this is reflected in the IETF. And we observed that it doesn't. The blue ones are responses from the US to the community. The red ones are China to the community, Europe in green, and the rest of the community in brown. We observed that in the IETF, we have really neutral to positive sentiment replies in the community. So we observed that no, if we have geopolitical

tensions around the world, in this technical community, we don't. They move towards having neutral conversations.

My takeaway on this plot is that the more data we have around the conversations, we can start predicting which ones can result in publication. Right now, our takeaway is around 70 to 80 messages. We can start associating patterns to which one will result in publication.

My takeaway is here. The IETF has recurrent temporal and sentiment patterns that have shifted over time and show us how the deliberation process has worked. The sentiment of replies has gone from neutral to positive, but also, there are no geopolitical tensions in the IETF, or at least this signals us that it's a neutral community. And that these structures can be associated with which ones are more likely to end up in a consensus, in publication. Consensus, no consensus, it's another process.

Ultimately, during these two days in ICANN, I consider that this could be useful, not just to the community, but to the working group chairs as well, to give visibility on how the conversations are unfolding on the policy development process. Here we have a really diverse community, and we might have stances on agreement, disagreement, and maybe political tensions; we don't know.

But we can analyze, and this visibility gives us how is the community engaging, and it could be useful to the working group chairs to see what is happening, how to drive the conversation, and

this is a start to build on consensus, how it's unfolding. And thank you very much. This is all from my side.

CHRIS BUCKRIDGE

Hi, I'm Chris Buckridge. I'm an ICANN board member. I've been in various communities for a while. So thanks, Hugo, for this. I think this is really interesting and important work because we have to look at these multi-stakeholder policy development processes as systems, and I think we really need to focus a bit more on understanding how those systems work, how they evolve over time. The IETF is obviously quite distinct from ICANN, and I think that your last few slides are noting that, but in another sense, the IETF probably offers a slightly more rigid, maybe, or static sort of system that we can look at and think about how that translates to ICANN.

There are a few things, well, there are any number of things that jumped out, but one that really jumped out to me was the shift towards more discussion later in the process. If it translates to ICANN as well, something to pay a lot of attention to because obviously the later people come into a process and provide their feedback, provide their input, the more difficult it can be to then go back and start at the beginning or start and rework things. So it's important to have those opportunities later in the process, but it also, it benefits everyone to come in earlier in the process and then be part of it. So I think just understanding if that shift is happening is really useful. So thank you.

HUGO RAMIREZ

Yes, thank you very much. So the idea is to do this analysis on ICANN and to see the trends that happen as well. There are multiple factors why the IETF is moving towards late conversations, but also because of context. So, three to four years of development, no one is looking to what has been discussed in the first year. But we can leverage also with LLMs to give summaries, to analyze, to have stances. But the idea is to see these trends and how the community is evolving. And having this, we can start to know how we will attack the consensus and speed of the process. So that's the idea. It's a start.

HISHAM IBRAHIM

Hugo, thank you for the presentation. Hisham Ibrahim, RIPE NCC Chief Community Officer. This is very interesting work. We at the RIPE NCC, we've done similar work where we've looked into sentimental analysis of policy discussions over the past 30 years. The idea was to see how the community mobilizes and reacts to different topics, and when they do and when they don't. Also, for topics related to legitimacy, is the community active? And for very various reasons.

We've done this work, and it was very well received by the community. I also know the IETF was interested in the work that we did, and they're asking my colleague that's done this to do that work. So I think since you've done work like this on the IETF, I don't know if you're in contact with them, but if you're not, I might be

able to put you in contact with people, because I know they're looking to do exactly what you're trying to find here.

HUGO RAMIREZ Yes, thank you very much. Yes, we can have a talk at the end.

JOHN CRANE So I had a bit of a methodology question, because I didn't quite understand the nuance. When you say it's a later conversation, are those new entities or individuals coming into the conversation, or is it just the amount of conversation? I participate in the IETF; many of my staff do. We are early, we are middle, we are late. And the input we give into the conversation really depends on where the complexity is and where we get to pushing that consensus around details. So I'm wondering whether new people or the same people across the thing would make a difference, and I wasn't sure what your methodology was.

HUGO RAMIREZ Yes, so regarding the late conversations, these are where most of the messages happen. So in three plus years, they're happening in the last year of development. I don't know specifically if the share of new people jumping in, jumping out, but we've seen that this is also because the draft is more mature, so when it's later on, it attracts more attention.

JOHN CRANE

In this world of PII, I don't know if you can still actually see who's behind each thing, but I think that's an interesting data point. Because I know my guys, they're spread right across that spectrum. So, yes, that could tell you that getting to the final consensus takes more interaction these days, but it could also tell you that there are new people coming late to the game, so it's interesting. And we have an IETF liaison on the board who I could happily introduce you to, and there are members of the Internet Architecture Board, etc., walking around, so you can get to meet these people this week.

HUGO RAMIREZ

Yes, thank you very much.

CHARBEL CHBEIR

Hola. I have a question. You mentioned that ICANN and IETF published these outcomes, okay? How do these two organizations coordinate to ensure their policies and technical protocols do not conflict or overlap? And now we have RIPE NCC.

HUGO RAMIREZ

So ICANN, RIPE, and the IETF have different objectives. ICANN is assigned names and numbers, and IANA has all the numbers. IANA gives these to the regional registries, which are RIPE, LACNIC, and the different operational registries. The IETF works more on the technical side, on protocols that make the Internet work: HTTPS, TLS. They have conversations because they are members of the

IETF. Overall, in the objectives, they work in different perspectives, but I don't know if that answers your question.

CHARBEL CHBEIR Yes, because I know the answer.

FERNANDA IUNES Okay, thank you so much. With that, one more round of applause for all of the presenters today. Thank you all so much. You did great. Thank you all for being here, and we conclude this session. Thank you again to our interpreters and our tech team as well.

[END OF TRANSCRIPTION]