ICANN84 | AGM – How it Works: IROS and IANA
Saturday, October 25, 2025 – 10:30 to 12:00 IST

SIRANUSH VARDANYAN: Thank you. Fernanda, if you can go through the scripts, please.

FERNANDA LUNES: Hello and welcome to the IROS and IANA session. My name is Fernanda Lunes and I am participation manager for the session. Please note that it's being recorded and is governed by the ICANN Expected Standards of Behavior and ICANN Community Anti-Harassment Policy.

Please observe the following guidelines to participate in this session. I'll also post them in the chat for your reference in just a few minutes. Only questions posted in the Q&A pod will be read aloud during the session as time permits and when directed by the chair of the session. If you wish to speak, please raise your hand in Zoom or otherwise as directed. When speaking, please state your name for the record and speak clearly at a moderate pace. If you would like to speak during the session, please raise your hand in Zoom.

When called upon, remote participants will be given permission to unmute in Zoom. On-site participants will use a physical microphone to speak. 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.

Interpretation for this session will include English, French, and Spanish. All are welcome to use the chat. Please note that private chats are only possible among panelists in the Zoom webinar format. Any message sent by a panelist or a standard attendee to another standard attendee will also be seen by the session hosts, co-hosts, and other panelists. I will now hand the floor to Siranush Vardanyan.

SIRANUSH VARDANYAN Thank you, Fernanda. Welcome again to the first session where we will learn about what is IROS and what is IANA. This is an important-- So, as I mentioned during the first session before this, we have in ICANN, there are two pillars, technical and policy development. And this first session is very important for us to learn how technically everything works. And the team who is behind this, it's my great pleasure and honor to welcome the Chief Technology Officer, John Crane, who is here with us, who will talk about the Identifier Research Operations and Security Function, which is IROS, behind this abbreviation, and Marilia Hirano, the IANA Director, and she will talk about what is IANA and how it works.

And please, this is an interactive session and not many of us are technical people, so please ask your questions, raise your hands, I will be facilitating here and Fernanda will be facilitating for our

remote participants. And without further ado, let me give the floor to Steve... John. Steve came up. John Crane. Yes, please, John. The floor is yours.

JOHN CRANE

Thank you. I'm going to use the hand mic because I realize when I'm sitting here that I can't see some of you, which means you can't see me. So, my name is John Crane, I am a Senior Vice President and the Chief Technology Officer at ICANN.

So, assuming you all know who ICANN is because you're all here, so we're not going to go into that. How many of you are here for the first time? Okay, quite a bunch of you. There's a lot of people, faces I recognize and a lot that I don't.

So, firstly, obviously, welcome to your first ICANN meeting for those new people and you're one of many if you've been coming here for a while. First piece of advice, just go talk to people, don't be shy, right? We're all nice, well most of us are nice people, but we're all willing to talk to you.

So, as the Chief Technology Officer, and I'm going to apologize because something changed last week, which kind of changed the presentation a little bit, we used to say that we are responsible for the research operations and security around the Identifiers. So, you will hear this term, Identifiers, Technical Identifiers, Unique Identifiers, quite regularly in the ICANN realm.

Most of the time you will hear about domain names, right? Everybody thinks ICANN domain names, and Marilia will talk a bit about this, but domain names are just one of the Identifiers used on the internet and to the technologists, they're not even the most important, right? There are IP addresses and other things that the network actually uses rather than humans use, which is what domain names are.

So, up until last week, my remit as an individual SVP was really about that research and the registration and operation of the Identifiers, making sure they're registered properly, making sure that the ecosystem stays secure, stable, resilient. As of last Tuesday, I think, I'm now also responsible for all the internal operations of ICANN, so all the technology you're using today, and all the technology our staff use, and all of our infrastructure.

This talk is not going to be about that piece. If you want to hear anything about that, ask me in about three months once I've figured it out, because it's brand new, not a new role, but back in that role after many years. So, let's go to the next slide, if we can.

Okay, so the function of IROS, we like acronyms, it's what we do at ICANN, it's what we do in the technical world. We really do like to initialize everything, so technically they're initializations, a lot of them not acronyms, but you know, I'm an engineer, so I get geeky on this stuff. I now have three pillars, because I have that internal engineering pillar. The other two pillars, which I still have, are the Office of the Chief Technology Office, which is all about collecting

data, doing research, and pushing that information, including things like training on technology, out into the ecosystem.

So, one of the things that we want to do at ICANN, and frankly in any policy forum, is you want to create informed policy. So, that's why what we do is important. We put the data and the facts around the Identifiers into the ecosystem, so if people have a policy question and say, how will this affect the technology? Does the data support what we're saying? That's where we come in.

The other side is that actual registration of Identifiers. So, if we're going to do a domain name, and we have what we call top-level domains, and I'm not going to get too far into it, because we really will talk more to it, somebody has to register that top-level domain somewhere, right? There is a database somewhere. This is literally how boring our job is. We keep databases, and there's one of those databases is, what are the top-level domains? What is the technical data associated with that? There are many, many more databases that we keep, but fundamentally, that is the core role of keeping the Identifiers unique and making sure the internet works, and that is the role of the Internet Assigned Numbers Authority, which predates ICANN, goes way, way back, and Marilia will talk to that later.

Next slide, please. So, we have on the office of the CTO side, different departments inside the organization. Now, we're early in the week, so the staff that are going to join us are not all here. I

think I have a couple of staff in the crowd. If you want to stand up, I can see you both, so don't just sit there.

So, one of the things we do is what we call technical engagement. Operations is kind of self-speaking. It's really about making sure that we function as a group, that paperwork gets done, that we have budgets, and all that kind of stuff. Technical engagement, where both of these gentlemen work in, is about pushing out that technical knowledge about the Identifiers, teaching people about what it means, in some cases, teaching people about how to deploy new technologies.

Research is exactly what it says, and we have two research departments, and I'll get into all of this a bit more. One that is really, the way I look at it is it's really focused on the protocols, and understanding what protocols we need. Has anybody heard of the Internet Engineering Task Force? All the tech guys nodding their heads. So, those are the guys that are really involved in that kind of stuff, and the other side is really our security research, security and stability, which is really doing a lot of research on how do you measure security issues and misuse of the Identifiers. And I keep saying Identifiers because it's not of the Internet, it's of the Identifier space. That is ICANN's remit. We do not run the Internet.

Anybody told you we do, they lied. Nobody runs the Internet. Not ICANN, nobody. It's run by lots and lots and lots and lots of network providers. Next slide, please.

So, technical engagement is managed by a gentleman called Adiel. He didn't manage to make it in yet. So, why do we do this? Part of it is about keeping relationships with other technical organizations. So, I mentioned the IETF. All those protocols you use on the Internet are developed at the IETF. IP addresses are distributed by something called regional Internet registries.

We call these our technical partners or technical organizations, and there's many of these organizations, and TE, or Technical Engagement, engages with those around technical matters and liaises with them. And it really is, it's kind of the framework of how we interact with that part of the world. It's like, who do we need to interact with? How do we interact with them? IETF is always my favorite example.

In the IETF, you often interact by going places and writing documents, right? That is one of the key ways that as an individual, as an engineer, you interact with the IETF. When you are writing a request for comments document, that is one form of interaction. But we also need to go and talk to the leadership at times or to the Working Groups, right? Each of these technical areas, and I know we really just came back from an RIR meeting, they have their own specific ways of working, and it's often my group that interacts with all of those technical organizations.

We have a pet project, favorite project, if you like, we call KINDNS. It's meant to sound like the English word kindness. Has anybody heard of manners? Right? Manners is a program by an

organization, one of our technical partners, called ISOC. It's about improving the ecosystem through working with people doing routing, which is a technical thing you need to do on the internet, and making that more secure through best practices. So, we thought if we can have manners for routing, why can't we have some kindness for the DNS?

So we can, if you want a good running internet, you need both manners and kindness. Also true for everyday life, right? So, kindness is our DNS norms, best practices platform, where if you are a operator operating DNS, you can go in and look at what we think the technical partners, it's not me and my staff, it's a community thing, and go and test your infrastructure to see if you're actually doing those things.

A little bit of testing processes, too, because processes are really important to technology, making sure you're doing things in the right way. But that's a pretty big project of ours, and, we like it because it's got a nice name, and we can do fancy swag, we can have nice t-shirts, we can make jokes about having manners and kindness, all that kind of stuff. Next slide, please.

So I talked about training. It's a pretty big part of technical engagement's role. We have staff in all parts of the world. Yazid works in Africa, lives in Africa. Champika works a lot in Asia and the Pacific, still lives in Brisbane, I believe. Yes. So, lives down in Australia, and we have people in Latin America and the U.S. and Europe, et cetera. So, that's how we do it. We try and put people

on the ground who understand the local environment and know the local technologists and can go out and do training and capacity development programs.

We also have an online training platform. Has anybody here used ICANN Learn? Anybody who didn't put their hand up, I suspect you didn't do all your homework, right? Let me try this again. Has anybody here used ICANN Learn? All right. That's better.

So there are technical elements in ICANN Learn. There are also, like, I guess laboratories is the best way you could call them, online platforms where you can actually test things. That's mostly run by our group, the technical side of it. There are lots of other things in ICANN Learn, which some of you didn't admit to going to earlier. I think Sharon is going to have a discussion about that. And, of course, as I said, just that broader engagement with the wider technical community.

So if you are a technologist and you're going to a network operators' group, how many people here attend NOGs or network operators' groups? There's a few. Chances are you will bump into our people. Because who runs the internet? Network operators run the internet, right? They're the people that actually plug in the fiber and they're the people that manage the routers.

So we spend a lot of time both participating but also in supporting network operators' groups. Very important community. And we'll support them on pretty much any topic related to Identifiers. A lot of it is DNS. DNSSEC is an obvious one. But also, if I'm an operator

and I'm struggling with what does IP version 6 look like for me or what does RPKI look like for me, you can talk to one of our guys and they will happily have a conversation with you. Sorry, guys, for giving you extra work. But happily. That's what we're paid for. It's what we love doing.

We also are involved in some of the advisory committees. So, this week you are going to learn about the way we develop policy and the way we receive advice. And you'll see the security and stability advisory committee. You'll see the root service system advisory committee. Those are two very technical committees. And we have staff that are liaisons, which really means they're sort of on that committee, working with those on a day-to-day basis. So, very close to those two particular committees.

Universal Acceptance. If you're interested in the internet or Identifiers in other character sets than ASCII, there's a steering group for that. We are also heavily involved with those folks. So, wherever there's a policy intersection that requires advice or knowledge about the technology, that's where you'll find us. That's kind of specifically our role.

The other thing that we do, and I think one of our guys may be off doing this today or if not, it's later in the week, is we do the same kind of outreach and education to a non-technical community, and that's law enforcement or the judiciary. So, we will do a lot of training and outreach to help them understand the internet and to help them understand how policy is developed.

So while we are technologists, we all also have to understand the policy environment and the world around us. The internet, while run by the network operators' groups and the network operators, is not just about technology. It's a mix of technology and policy. And being here at ICANN, you are right where those two things meet. So, my group specifically is really, really at the nexus between those two issues. But if you're interested in either of those, or even better, both of those, you're at the right place.

Let's go to the next slide. So, these are the folks that are out there. We're actually hiring two positions. I don't know if they're filled yet. We're working on it. We're hiring another position in Asia Pacific and another position in Africa. So, these are the five that are currently out there and deployed and working really hard. Apart from the two guys are just sitting in a meeting listening. But the rest of them are out there working hard today. And we are trying to add two more people.

Asia Pacific is a rather large area and the African continent is a rather complex area. It's also large. There's a lot of countries there. So, that's why we're going to double up and put more resources into there. Go ahead. Pictures of people doing things. All right. I mean, it really is, right? It's just here's pictures of us presenting stuff. It's what we do.

Research. So, I've talked a lot about this. We mostly engage with the DNS technology folks because those are the folks that are often

more connected to what ICANN does. But we also engage with folks in the routing technology areas and others.

Take a drink. So, there's a lot of research goes on and we talk about that a lot. So, you may not be aware or you may be aware. How many of you have been told what root servers are yet? How many of you know what root servers are? Okay. So, you've not had that discussion from the RSSAC. So, ICANN manages one of the 13 DNS root servers. So, because we have access to that, we have access to the query traffic, which means we can do research on it and we can look at the way root servers are being involved.

We worked very closely with the other root server operators and with the DNS research community. That's actually a very specific community. Sort of understand what the ecosystem is, to understand where it needs developing, to understand the threats.

Anybody ever suffered from a DDoS? A few of you. Very annoying. Well, it's a piece of infrastructure. It gets DDoSed on a regular basis. We survive them. But, we need to understand why. So, if you DDoS, sorry, I'm doing acronyms, distributed denial of service attack against a piece of infrastructure, 95%, and this is a number I made up, it's not based on research, of them seem to be just misconfigurations. Right?

So, when we see a large spike in traffic, we need to do some research to figure out who changed code where. So, my guys may phone up somebody who has a large operating system or a widespread operating system and say, hey, did you guys do an

update? Because we're now seeing millions of queries coming to the root servers that look a lot like they're only coming from your operating system. And they'll go, oh, we didn't test that. And then we get it fixed. Right?

It's not a threat to the ecosystem. We have plenty of capacity. But when we find those kinds of things through our research, we're able to go to the code providers, sometimes it's browsers, sometimes it's operating systems, and say, we can see you made a change. Were you aware of this effect? And then they can fix it. You'll almost never see that anywhere in press releases or anything like this.

It's all stuff we do in the background. We do a lot of working with that DNS technology industry in the background saying, hey, we discovered this. What can we do? And sometimes they'll come to us and say, hey, we discovered this thing in the ecosystem. We go research it. That's what this group does.

Next slide. So, some of our activities. We measure the concentration of infrastructure. How infrastructure is used. There was a lot of discussion at one point about many of you may have heard this term, digital sovereignty. And then how that affects DNS. So, a lot of research saying, everybody in our region or in our country is using this large public DNS resolver. It's bad. It's terrible. And then we go and do research and go, actually, no. This is how your users are querying the DNS. And we can see it because we can get access to the traffic. And you made an assumption about how people were using the DNS, but it doesn't actually match reality.

So, we try and bring the facts and the data into the discussion. Because if you think that's reality, you are going to make policy choices and technology choices based on that. So, we've published documents on some of this stuff saying this is how it's actually being distributed. Our job is to bring data and factual information into the policy discussion. So, when we see those kinds of issues, we try and go and do this.

DNS error reporting. The error reporting, if you're a technologist, you care about this, how you find out there are faults in the ecosystem of the DNS, it kind of sucked. It wasn't very good. The protocols weren't in place. So, some of our staff went to the IETF, Internet Engineering Task Force, and worked on developing protocols to make error signaling in the DNS better. It's another thing we can do.

We can go and influence the protocols and the technology to make it more secure and stable. And I talked already about being able to measure the behavior of the root servers. The final one there is a metrics platform, ITHI. We gather metrics from around the internet and publish them. It's not our data. It's people telling us what they're seeing on their network. So, it's kind of a place to go and get a view of how the network looks in various places. So, you can go see which ISPs getting how many DNS queries, things like that. Next slide, please.

And we're losing half the slide, but that's fine. And next slide. I talked about this. This is the fourth group. These are our guys

looking at how the Identifiers are used and misused. So, these are also slightly different set of characters. So, you can sort of note the characteristics of the people depending on which group they're in. The folks doing the engagement tend to be extroverts. Right, guys? They like going out and talking to people. They're chatty. They're good communicators. The folks doing the Identifier research and the protocol stuff, they tend to be engineers. Very good engineers, I'm glad to say. But engineering types. And the folks doing this tend to be academics. Right?

So, they're more academic researchers. And that's deliberate. Because that allows us to put them in a room together and get the best of all the worlds. So, when we put out a paper, you will know that the engineers have looked at it, the academics have looked at it, and the people that actually have to go and promote this have looked at it. The people actually can communicate. So, it makes a better white paper, better documentation, better output.

So, at the moment, the big topic that you will hear about in the community, which is a policy discussion, is something called DNS Abuse. Has anybody heard that term yet? It's not about shouting at the DNS and abusing the DNS in that way. It's about technical abuse. Things like phishing and malware distribution using the DNS, et cetera. And we measure that.

So, we have tools that look at the DNS namespace. We take in from the generic namespace all of the zone files. Zone files are where we keep the data about what's in there. You can imagine the one for

something like .com is massive, because they've got millions of registrations and some of them are smaller. And many for the ccTLDs. We have a lot of partnerships with ccTLDs. So, we have a good view of what names are in the DNS.

Not what names are registered, but what names are actually in the DNS and how people are telling us that they are being misused. There are many data feeds out there that will tell you whether a name has been flagged for malware, for phishing, et cetera.

So, we have a system that we designed years ago, there are other people doing this now, that will measure that and allow you to look at a particular TLD, top level domain, and say, oh, 3% of the resolving, well, actually 3% would be really bad, but 0.3% or 0.03% of the resolving names in this particular TLD have been flagged as abusive. Data we didn't have years ago.

The main reason we did this project, and this is going to sound counterintuitive, was not to measure those things. The main reason we did it was to promote the science, to demonstrate that there are methodologies you can use to measure these kinds of things, and you can build tools to do this. Because there were many people saying, well you can't do this.

So, the worst thing you can ever say to an engineer is, it cannot be done. Because we will prove you wrong. We will find a way to do it. And that's kind of what our role is, right? We are pushing data, we are pushing facts, but the third thing we are pushing is the science. So, you will see papers about how to measure certain

things. So, every time we do something like this, we're a not-for-profit public benefit organization. So, we don't care about the intellectual property. We will tell you exactly how we do things, we will tell you exactly what data feeds we use, we will tell you exactly how we look at that data, and how we do deconfliction.

So, all of our science is pushed out there. So, if you are in one of these businesses that are measuring this kind of thing, take our science. Have at it. Improve it. Tell us that you've improved it so we can improve ours. That's another role that this group specifically does, is pushing the science around measurement of issues on the internet. And of course, educating the community about that. And we've funded a couple of outside research projects.

There's a research project out there, for example, called INFERMAL. It was done by a university in France which was trying to look at the elements that drove abusers, bad people, to do particular behaviors in the Identifier ecosystem. Not our area of expertise. An area that the community was interested in from a policy perspective, so we managed to fund that particular piece of research. Very clear it was their research, not our research. We just funded it. And then we could help them by saying, well these are the kind of questions that are being asked by the community. This is the kind of policy interaction we need from this document.

So, all of these people are very busy. There will be people from all of these groups here though at ICANN meetings. Unfortunately, we

don't get our own little 'I'm a geek' thing. I wonder if there's an 'I'm a geek' flag. We'll see if we can get some 'I'm a geek' flags and then you'll be able to find our folks. Well, I guess there's probably lots of geeks here. We won't be the only ones. And we'll talk to you about all of these. So, here's some of the key activities that that group is doing. The academics.

Who's heard of Domain Metrica? That's our measurement tool. We used to have a tool called DAAR. That was the first time anybody had done that. And now we've evolved and we've built a new one because we're trying to push the science. INFERMAL, I talked about. We didn't do that work but somebody else did. We really like try to look at things like, what's the implementation of an active domain? What does it mean for a domain to be active? Because there are things like parked domains, right?

Parked domain is a domain that is active but it may or may not be harmful depending on which one it is. So, we published an IEEE white paper on that. Remember these folks are academics. So, you'll see a lot of our papers will first go through academic peer review. This is exactly why we do it. We send it to these conferences because it's much harder to get published at one of these conferences than it is to publish it yourself.

Once again might sound counterintuitive but remember we're trying to push the science. So, if we can take it to somewhere like IEEE and have them allow us to go through that path, it just makes it that more rigid. We did a classifier. Who's ever heard of

something called, what do they call it? AI. That's it. Artificial something. Or as engineers call it, machine learning. So, we used a machine learning platform to classify unsolicited email.

So, take millions of emails that somebody has classified as unsolicited email or spam and actually take a look at that and see if you can actually classify what kind of abuse it actually is. The reason we did this was because we were seeing a data feed with millions of names from emails being associated with phish and we're really interested in phish. It's one of the things that we would classify as DNS Abuse but we didn't quite believe it. Right?

Just because somebody says something is a phish doesn't mean it's a phish. So, the thought was could we actually take Artificial Intelligence or machine learning, build an LLM and actually take these hundreds of thousands of emails and classify what kind of abuse they were. Not because we wanted to classify them but we wanted to push the science.

So, we've issued a paper. You can get the code we used. That went through Trustcom, another academic area where we had to go through academic review and we've we used the APWG data in that and we presented that paper and once again, we don't care about the intellectual property. If you're interested in it go read it, replicate it, improve it. If you improve it let us know.

The reason we really did it was because people told us it couldn't be done. So, we did it and it's pretty cool. Very proud of the guys that worked on that. Has anybody heard of Reputation Block Lists?

You probably will do although it's a kind of technical thing. It's also kind of a policy thing. These are lists of what names you should or should not allow to resolve, what domain names.

We published a paper on understanding the quality and the value of those lists. Because every time you do a piece of research based on RBLs or Reputation Block Lists, somebody will tell you picked the wrong list. But I don't like that list. I do like this list. So, our folks said, well we could probably put some science behind that and actually demonstrate how we choose lists. And every year we look at the data we use and we put them through this process now and we decide whether or not we're going to keep using those lists.

And if we get a new set of data, we now have a set of criteria and mechanism for actually evaluating the value of that list. Sounds obvious, but nobody had really done it and it just occurred to us that somebody should. So, that's the kind of thing we do. We've done a lot of looking at blockchain names. What do they mean? How do they actually work? If you're interested in Blockchain Technology and Namespaces go talk to the people that are developing them and you will quickly find that there's a lot of not misinformation but lack of clarity about how some of these works.

They are all pretty well not all of them but most of them are actually individually developed they're separate development paths. So, there's not no such thing as blockchain names in a uniform manner. So, we try to understand that because it intersects with the policy world. It's like if a name in a different Namespace, that's

how we relate to them, looks the same as a name in the DNS space, what are the implications?

If it behaves the same as a name in the DNS Namespace, i.e. you can type it into a browser and it will resolve to something not through the DNS but through some other technology, what are the implications for that from a trust and safety perspective, from an end-user perspective, from a technology perspective of how applications are going to actually handle those kinds of things.

So, yes, we are geeks and that is exactly the kind of stuff that we do. So, OCTO documents, Office of the Chief Technology Officer documents, I write none of these. This is actually written by smart people and they're on all kinds of topics. If you think there is something that we are missing, i.e., there's this really fascinating Identifier related thing that's coming up and for some unknown reason we've missed it or not thought about it, come talk to us.

We will either explain to you why it's not relevant, which happens a lot, or we'll go, oh, we should go do a study on that and release a paper. These are just some of them, I'm not going to list them out, go to the publications page. It's on a wide variety of things, some of them are slightly more policy oriented than others. I mean one of the most-latest one is random candidate selection for elections.

Why did we write that? Because there was an interest from people in the community from the policy world of, can you use technology to randomly select your candidates and that you want to put on committees or boards etcetera and it turns out there is and we have

engineers that like things like randomization and they figured they'd go write a document and we let them because it's cool. So, yeah, we're the geeks. I think that might be my last slide.

Now, we talked about that, yeah, we have blogs, we have speaking engagements, we do trainings, we're here. So, you can't push ideas and technology and data, if you're not external. So, that's the office of the CTO as it was a week ago and now we've got to run all the servers too. So, do you want to do any questions on that now, Siranush, or do you want to move forward?

SIRANUSH VARDANYAN Yes, we can take one two questions if there is any or if not, we'll go. Yes, I think Maciek will go first with you.

JOHN CRANE Hi, Maciek.

SIRANUSH VARDANYAN And then Seth, and then done. Oh, okay, one more here, three, and then we'll continue. Maciek, go ahead.

MACIEK PIASECKI Hello. Maciek Piasecki. I'm a fellow with ICANN and a cybersecurity educator. That's a real job according to the European Union and you've mentioned that you want to build capacity and communicate. So, I wanted to ask to whom you want to

communicate. You've mentioned that you treat the law enforcement but is it also the end users? Is it the government?

JOHN CRANE

We tend not to go to the end user level although we know we work with ISOC etcetera, who do focus more on that. So, network operators, DNS infrastructure operators. One of the areas that we struggle to get more of a grip in is the telecommunications industry which is different to the internet industry.

So folks that are in there with policy developers. We provide materials that do get to the end users. I mean it depends on your definition of an end user right. So, I would argue that we're all end users. So really, it's about the people able to influence the policy and the people able to influence the technology, and end users typically aren't in that, if they're a pure, like my sister-in-law is an end user but she's not influencing the policy or the technology. So, that's what we're trying to influence by having people more informed and if you have ideas how we can do that, talk to these guys.

MACIEK PIASECKI

So, just a little follow-up. So, what are the hottest topics you are trying to communicate right now?

JOHN CRANE

So, there are various this is another area that we don't really talk about. So, there are always hot topics generated by papers coming

out of policy bodies. One of the more recent ones was a push for RPKI which is A Routing Public Key Infrastructure from governments to put that into legislation. Yeah, okay, and I will slow down for the interpreters.

So that's something that comes out of legislation. I probably read a couple of dozen legislative papers a month and then we want to educate them about how the industry actually works, how their proposed policy may or may not break things. So, that's always hot. I mean RPKI was one of them recently. There are some policy papers out there. I think the WEF has one which is around improving security and some of the things they're suggesting you do in there may not actually work in the real world, because operators aren't going to be implement them.

And then from the ICANN side it's the new technologies. So, obviously KINDNS is one of our projects that we're trying to get people to follow the best practices. But also, DNSSEC, sometimes IP version 6, sometimes helping people understand what is not our job, is as important as them understanding what is our job. I think two weeks ago, I was in the Middle East on a panel talking about artificial intelligence. And there is a conception that all technology somehow has massive implications for the policy.

And while they do all have implications, they're not all as massive as people think they are. And also, sometimes it's about explaining to them that ICANN's role is about the Identifiers and not about these other things. So, that regularly becomes a hot topic and it's I

said Artificial Intelligence but it's whatever the new buzzword is in technology.

So, we spend a lot of time trying to damp down their enthusiasm for bringing that into the ICANN world so that we can focus on what we are. It changes all the time. Some of that comes out of what folks like SSAC and RSSAC are telling us. So, if SSAC is telling us a piece of advice that is a particular like they did with DNSSEC then we'll go work on that. So, I don't think there's a straight answer if it's this or that. It changes over time. Some things are constant like trying to secure the DNS, DNSSEC, trying to secure routing, RPKI, DNS BGP, things like that.

SIRANUSH VARDANYAN Thank you. Seth?

SETH ADJEI GYIMAH Okay. My name is Seth Gyimah from Accra, Ghana, University of Ghana to be precise. So, my question is centered around your functions as IROS. You mentioned that your functions were two, the OCTO function that involves research data collection and then the IANA functions. But not long ago there's been another addition, the internal engineering, where you're going to handle technology infrastructure.

In the past, I know your functions are already-- you're overwhelmed because you said you are even employing people, technical engagement team to Asia, Africa. You're already

overwhelmed. Now there's an addition of handling technology infrastructure. Big thing, big in addition to your functions. So, my question is why wasn't this new function assigned to a different team or unit?

JOHN CRANE

You need to ask my boss that. So, what we actually did is we bought in a CIO, right? So, it is a standalone function. What we have in ICANN, we have our senior vice presidents that are the executives. So, if you ever get into a, it's not a technology thing, this is a career thing. Executives don't always focus on the day job, right? They have people that focus on the day job.

So, if you were to ask me which slide something in one of these guys' presentations was or what they were presenting in a particular place, not my job to know. They have a manager that does that. So, the same in IT, we bought in a CIO. I will be the executive for that, which means I will be giving them strategic guidance and helping them navigate the world. Why they put it to me instead of somebody else, I think my boss doesn't like me or he thinks that I can actually work there to make it function correctly as an executive. I will not be getting an enable on the routers. I will not be getting a password on any machine. They barely let me have my own laptop.

So, it's an executive role. It's quite normal in organizations to split that way. And as you get further up the leadership chain, you get to do less fun stuff. You occasionally get to talk about it like this,

but you end up working more on strategy and strategy implementation than you do on the actual technology. I hope that answers.

SIRANUSH VARDANYAN Thanks. We'll take one more question now, but we'll come back. We'll come back at the end for the questions. Okay, Shashi, we'll come back.

SHASHI RAJ Hi, I'm Shashi Raj from India National Finance University. I'm a master's student. I'm in my final year. I have three questions, but you can answer anyone that you like.

SIRANUSH VARDANYAN Very, very short questions, please, because we don't have time.

SHASHI RAJ Yes, ma'am. So, my first question is when attackers try to use the attack of DDoS, they query from the DNS from the domain name. But what if it happens from the IP address directly? They will not go in the DNS query. Second, what's your view on the recent AWS failure? Can you give some points on that? And third is, what are the other attacks other than DDoS that are very critical for internet?

JOHN CRANE Okay, three very different questions.

SHASHI RAJ Thank you so much.

JOHN CRANE So I can actually probably answer two of them in one. So, all DDoS come from an IP address because every machine has an IP address, right? So the question is, which protocol is it using? IP addresses are not a transport protocol. They're purely an Identifier. If we see a lot of, the real question often is, is it TCP based or not? So, DNS is not. So, it doesn't really matter where it comes from. And it's not all these attacks are not all against DNS infrastructure, that's what we care about.

So DNS has been used in a manner where you can actually generate larger packets by sending smaller packets. So, you send a small packet to a DNS server, it answers somebody else with a larger package, a larger packet. That's called a DNS amplification attack. That one is kind of specific to the DNS just because of the way the DNS works. But you can use pretty much any protocol to do it. DDoS, right? DDoS is exactly what all you're doing is overwhelming the link or the connection.

So as long as you can generate enough more traffic than that system can use, it doesn't really matter which protocol you use. We see a lot of NTP attacks, we see a lot of DNS attacks, but there are plenty of others. On AWS, which is the only thing of it, I think they did a really good job communicating it. So, go read this morning's

message from them where they've actually explained what happened.

It was their infrastructure, their problem, it wasn't, the internet didn't go down, the internet was still working, some services went down. There happened to be a lot of services, but the internet was still working, right? And they've done a really good job of explaining what happened within their infrastructure and kudos for them for doing that and being so transparent about it.

SIRANUSH VARDANYAN Thank you, John. John might leave this session after, yes, this presentation, but we have his team members, Yazid and Champika are here. But during this week, whenever you see John somewhere and you would like to ask a question, please stop him in the corridor and talk to him. He's really always welcomed the questions from newcomers in particular. But thank you, John. Thank you for being here and thank you for your time. And with that, I would like to give the floor to Marilia to talk about what is IANA and how it functions. Marilia, please.

MARILIA HIRANO Thank you. This is on, right? Thanks, John. He helped cover at least, I think, half of my presentation, so it's going to make it easier. Very, very, thank you. But if you want to stick around for more questions at the end, I just want to go quickly through this. And the reason why is, on Monday, we have a special session where we're

going to go in depth into the origins of IANA and explain the importance of IANA in more detail and also where we're headed.

So, for today, I wanted to give a sense of just a brief glance of what it is we do. And as you move through the days at the ICANN meetings, especially I think by Monday, when you come to our session, you will have forgotten or things will have taken over your mind because it's a lot and a lot of you are new to this. So, maybe what I speak about here will be brand new on Monday when you attend that session. And I'm saying when because I'm pretty sure you will.

So, what is IANA? As John mentioned, IANA is the record keeper for these unique names and numbers that are used for internet technologies to interoperate. So, one thing that we always like to mention, and we will go into detail on that on Monday, is we predate, IANA predates, not we, predate ICANN. ICANN was created in 1998, and the IANA functions have been around since the 70s.

So, the Unique Identifiers include, and John mentioned a lot of them, protocol parameters, internet numbers, which are the IP address, and domain names. And IANA, we maintain these records and just maintain, and it's important to stress this, according to the policies that are adopted by the communities. So, we do not set policy, we do not make decisions around policy, we just implement the policies.

So, John also mentioned this, so this is quick, coordinating these unique Identifier systems. Without that coordination, the internet

wouldn't interoperate globally as it does today. And if our connected devices don't use the same system of Identifiers and numbers to talk to each other, this system won't speak a common language, so it won't work.

The authoritative registries that we maintain, these records, they're used by vendors, they're used by service providers, businesses, application developers, a lot of end users won't see this, but in order for the internet to work, they need to implement and they need to use these standards that we maintain. One example, a common one, if you try to type in a website and you get that 404 error or the 403 error, that's a unique Identifier, that's part of a registry that we maintain.

So, our core deliverables on the protocol parameter side, John mentioned a lot, the IETF, we work very closely with the IETF, our team attends all three IETF meetings and we talk to them monthly, we create new registries when they request it or we add new values to the existing registries. And as you see here, the size of the job, we managed about, there's about 3,000 registries that IANA maintains.

On the name side, we manage the top-level domains, assignment and transfers, and top TLDs, you're going to hear a lot about that this week, the naming function is the most prevalent here at the ICANN meetings, and we do routine maintenance of name servers and other technical elements of the TLDs.

We also manage the root zone KSK, yeah, thank you, which are key ceremonies, this is also going to be in our session on Monday, and then we allocate large IP address space, and John mentioned too that we work a lot with the regional internet registries, so IANA does not assign IP addresses directly to internet service providers, we work with the RIRs on each region, and that's why I was just at RIPE, which is the European regional internet registry, and we allocate large blocks to them, and then they in turn allocate to the ISPs.

And then we also serve as subject matter experts for the upcoming standard efforts when it comes to IANA registries, and we are bound by contracts, and I'll go through that in the next slides.

On who's involved, okay, so as you saw, we are under John Crane's team, and we are part of ICANN, the IANA department sits under ICANN, and you'll see here, the ICANN is responsible, is the organization responsible for the IANA functions, we have contracts, so ICANN contracts PTI, which I will go through too, to perform the IANA functions, so PTI was a not-for-profit affiliate of ICANN created after the IANA stewardship transition, so I'm just going to ask for a show of hands, who here is familiar with the 2016 IANA stewardship transition?

A couple of you. So, let me just briefly, before 2016, the IANA functions, we were under contract with the U.S. government, and in 2016, the work was transitioned to the global internet stakeholders. So, with that, a new affiliate was created to be the home of the IANA functions, but with the oversight of ICANN.

ICANN provides us with their legal team, the HR team, finance team. We all sit in the Los Angeles office at ICANN, but we are separate in that sense that we operate through the public Technical Identifiers, PTI. Next slide.

Yeah, so there you go. I mentioned this. So, PTI, it was created in 2016 to perform the IANA functions. Us in the IANA team, we are paid, our paychecks say PTI, it doesn't say ICANN, but ICANN is its sole member. So, it's an affiliate of ICANN with ICANN being its sole member. Then we, here's the PTI board.

So, PTI has its own board, separate than the ICANN Board. It's a five-member board. You'll see John's picture there. John is part of the PTI board, along with two NomCom appointees and two other staff members, which one is Kim Davies, who is the PTI president. And then we have Xavier Calves, who's the CFO of ICANN, and you probably met him or will meet him this week.

Then with PTI, we have the IANA staff. So, these are the 18 people who are responsible for delivering those services to the world. And I'll go a little bit about into what we do as a team. You can go to the next slide, please. So, the first is IANA operations. This is the core team that delivers all of these services, that actually go in there and make changes when we get requests to modify a registry.

So, if the IETF decides that through a standard that we need to modify a registry, they will come to IANA and say, we need you to make these changes and publish it through our databases. As John said, this is the boring part. We maintain databases, many of them.

And so, they will come to the IANA operations team. These are the IANA specialists. They're not here yet, but a couple of them will be here later today. So, they're the core service delivery team.

The next slide. Then we have our technical services team, which is our engineering team. So, we have software developers on the team. We have product management. We have the cryptographic business operations. They're the ones who manage the key ceremonies, which you will hear about on Monday. And that's the picture there of us inside one of the tiers of the safe. And that's in a key ceremony that you'll know more about. I'm not going to go into that. Not the team. No, that's everyone involved in a key ceremony.

Then we have my team, the IANA Strategic Programs team. And since John said it, not me, the geeks, we are basically the geek whispers. We are responsible for audits, compliance. We measure Customer Satisfaction, Continuous Improvement, Project Management, Community Engagement. And then we are also responsible for development and implementation of the Strategic Plan and Budget Process.

So, basically, I'm looking at her here because one of the RIPE sessions I attended, Laura, she mentioned something that I still remember. It was engineers don't like it when we tell them how to do their jobs. And they pretend they don't like it. They love it. And that's what we do. Through all of this work that you see here, of course, we have to go tell them sometimes how to do their jobs

better and to plan so that they can focus on being the brilliant engineers and go out there and explain a lot of the stuff that John was explaining to you that I could not do. But I can tell them what process to follow in order to get that job done. So, that's what my team is there for.

One key takeaway that I always like to have here, and I mentioned briefly, is what we do and what we don't do. So, again, we don't create or interpret policy. We don't determine what can be a domain name. So, we maintain, we manage the root zone. We delegate domains and make transfers as requested, but we follow policies. We don't create or we don't interpret. And we don't choose TLD managers.

What we do is create the registries based on policies from the community. We maintain existing registries. We allocate the IP address space to the IRRs, only in very special use cases that we will allocate IP address space to basically at the request of the IETF. And we publish all registry for general public use. So, if you go on IANA. org, you'll be able to see all of those registries in detail.

Again, we will go through a lot more of how IANA came to be on Monday at 3 p.m. and Siranush, believe it's on their schedule, right? So, you'll learn more about the history of IANA and why it's important. Explore practical examples of our work. Find out what we'll be working on for the next five years. And also, we want to invite you to, we're going to show some of our priorities, how what we're planning on and ask for your input.

So, here we want you to tell us how you're doing, what you thought of the presentation. And also, this one-minute survey allows you to give us input on what you would like us to talk about more, or if you have any venues that you think the IANA topic would be beneficial to come speak at. We are happy to receive that.

We love getting feedback because that really drives how we prioritize our work. And then I just put the pictures of the four of us who are here at ICANN84. So, you'll see us later at the fellows' social hour and come talk to us. We're happy to explain anything else that you want to know about IANA.

SIRANUSH VARDANYAN Thank you, Marilia. Thank you very much. And we have a couple of minutes to go for a couple of questions. Please note, before we move forward, all the PowerPoint presentations which are available and you can see during the sessions, they are available for you in the schedule. So, under each session, if you click on the particular session details, you will see uploaded slides. So, wherever you want to use them, feel free to go there and download and use it.

So, they are all publicly available. Don't ask me where to go and where to find the slides. They are in the schedule. Thank you. And we will move forward with the hands over there. Mayssam, you had the question. And then Chinar and I know Tinuade had here.

MAYSSAM SABRA: Thank you. My name is Mayssam Sabra. I am an ICANN84 fellow. So, it's really simple. Just I'm curious to know if you mentioned in your presentations that you conduct some research with communities on security and interoperability and resilience. Just I want to know if you support or collaborate with governments or regulatory bodies?

JOHN CRANE: So, support and collaborate are interesting words. We absolutely work with them. So, inside ICANN, there's another department called Government Engagements. And they manage the relationship, if you like, with governments. But then they bring in subject matter experts. So, if there are things that governments need, advice, information, whatever it may be, not just about technology, but about anything ICANN does, they work with the government engagement folks. And then they come to us and say, can you send us an SME? Can you do some training for us, et cetera? So, the answer is absolutely. But we arrange that through the government engagement team because they are more diplomatic than we are.

SIRANUSH VARDANYAN: Thank you. Yeah, Charbel, go.

CHARBEL CHBEIR: Hello, my name is Charbel. I'm a first time fellow, always a fellow. I'm a lawyer and cybersecurity expert. I'm president of Lebanon

ISOC chapter. So, I have for John a question, quick question. You talked about digital sovereignty. I want, and you raise up a very interesting point that I want to elaborate a little bit. If you consider a DNS as a key indicator for sovereignty or the data center? This is my question.

JOHN CRANE

We could spend two hours on digital sovereignty. So, digital sovereignty, for those that aren't aware of it, is often the discussion about controlling your own destiny within a country by having products and infrastructure often within your national boundaries, which I always remind people that the internet's a global thing.

So, it's much better to think about controlled from within, it's much easier. And I'm not a lawyer, but often it's the legal frameworks and the contracts that are the important parts. So, if you don't have mechanisms to store data within your national boundary, then you may not have mechanisms to apply local law to them. Right. That's one element of it.

And the same goes for every piece of infrastructure. It's like, what do you want to be able to have your say in from your national perspective? But how do you do that while balancing it with the global nature of the internet and ensuring that you have the resilience? Because while you may want to keep a lot of data in your country, you probably also want to keep some of it outside or

copies of it. What happens if you have an issue with your bandwidth?

You have some kind of, some major disconnection. How do people get to that? And your diaspora, your nationals, your community aren't always inside the country. So, digital sovereignty often gets broken down to very simple concepts, but it's actually really complicated. I'm happy to have conversations because I've had conversations with many governments about this over the years. It's not as simple as people think it is.

And then you get down to manufacturing, which is something that we really don't get involved in. How much digital sovereignty do you want? Now, you will see this discussion hit the newspapers this week because a large infrastructure provider, who happens to be a U.S. infrastructure provider, had an outage. And you will see the questions about, well, how do we control our destiny as a nation when we are using large scale, what we often call hyperscalers, that are based outside the country? And they say, well, we just build our own. Okay, so do you have the education in place? Do you have the systems in place? Do you have the infrastructure in place? Can you manufacture the equipment?

It's really simple on paper and really complex when you actually try to do it because the internet is a really complex environment. When you understand all the protocols and how it's worked, sure, it's simple. But once you start digging, it's very complex. And often in the digital sovereignty conversation, that part of it gets lost.

SIRANUSH VARDANYAN Thank you. Omer [ph]?

OMER [ph] Thank you, Siranush and John and Marilia for an insightful presentation. So, I have a question. Currently, or as of now, has there been any discussion in IROS or IANA about implementing blockchain DNS in the traditional DNS infrastructure, while ensuring that it is interoperable with the internet that we're currently using? So, for the record, I'm Omer, one of the Next-Gen participants. Thank you.

JOHN CRANE I get all the good questions. So, not directly. So, what we have had over the last years here at ICANN is a lot of technologies who are using ledger systems like blockchain come and explain to us what they're doing, as explaining to them how that will interact. Remember what I talked about earlier, how that will interact with the real world. We have registries that are interested in, within their zone, how they can use ledger technology, blockchain or other, to increase both security, but also the predictability of their systems.

Nobody's quite figured it out yet. But there are problems with, and I've explained this to many of blockchain folks, there are problems with the concept of immutability, the concept that you cannot remove a name, you cannot change a name because it is protected by the blockchain. It's not a technical problem, it's a policy

problem. So, remember, one of the things that we talked about in the DNS is how the ecosystem can be abused.

The policy discussion is all about what you do in that environment. If an Identifier name or anything is used for malicious purposes and abused in some way, what are the remedies? And in the early days, most of the blockchain people would come and say, immutability, you cannot do anything against this name, for good reasons often. It's like freedom of speech, things like that. And then you will ask them the question.

So, you have this used for something that's, we all agree it's abhorrent, some association with CSAM, child sexual abuse material, or child sexual abuse and exploitation material, but it's immutable. So, how are you going to do something about how that Identifier is used to solve that problem, right? And it could be some form of fraud, it could be phishing, it could be anything. But the question is, when you have a problem with an Identifier, because you will, how do you actually take action to disable or do some other action against that Identifier?

So, we've been having a lot of discussion with the folks from those worlds, and they've been fantastic, right? They've been coming here, they've been talking to us, they've been trying to understand their problem space and our problem space, and they've changed technologies. You will see some that were immutable, immutable, immutable, now saying, oh, we're putting policies and technologies in place.

So, it turned out they weren't quite as immutable as they said they were, because it turned out you could adapt the technology to make changes. So, we are not looking at doing a ledger system today. The blockchain stuff out there comes with scalability issues. Remember, the internet does billions and billions of queries every day. Much of the blockchain technologies, because of the way it authenticates things, will not necessarily scale to that.

And we have a lot of discussions about scalability with them, and they say, but we have 100,000 users. And we say, well, we have six or seven billion. How do you get from that tens of thousands, hundreds of thousands, millions to the billions? And when it comes about queries, the trillions of queries that you need to handle. So, a bit of a complex answer. Happy to talk offline. We're well aware of the technology. There are discussions with those technologists, but we have not made any plans today to introduce something like that. Doesn't mean we never will. And by the way, it won't be us. It would be the IETF, right?

Somebody would need to come up with a protocol to do this. But as of today, I've not seen any serious discussion about doing that. Certainly not at the root.

SIRANUSH VARDANYAN Thank you. Tinuade, please go ahead.

TINUADE ABOSEDE OGUNTUYI Thank you very much. My name is Tinuade Abosede Oguntuyi, ICANN84 fellow. I'm from Nigeria, that's West Africa. Thank you for all you do from the Office of the Chief Technology Officer. But I'm a bit curious, because recently I read that even the big fours are now really concerned about quantum computing. I know last year, I attended two road shows with the Coalition of Digital Africa and all that, and we were talking about this. What is ICANN doing just to show some form of readiness, either to train, since your office is also capacity building, so that we are ready for this and we don't play the catch-ups? Thank you so much.

JOHN CRANE So, oddly enough, we've posted a document on this. So, the area that is most intersectional with what ICANN and IANA does is post-quantum cryptography. So, how is cryptography going to look like once the quantum world is here? It's not here, right? That's the main thing to realize. I actually sat on a panel in the Middle East last week about this very topic.

And if you will find anybody here who works for security companies that do post-quantum, all right, I'll say this then. They will tell you it's here today. They will tell you need to be ready today to do this, because they are selling you an idea and a product. But our research has said you don't need to be ready today for post-quantum cryptography, but you need to keep a really close eye on the technology, because it will change.

So we regularly do new research. We actually use outside researchers for this, because it's, guess what, it's not our area of expertise. So, we consult with experts around where they think the technology is. We are looking at how are the algorithms for signing the root zone going to change? How is quantum technology going to affect cryptography? We just keep an eye on it. Now, I don't think we're planning to train on this at this moment, but if it becomes an issue for DNSSEC, then we will be training on it, right? We will be going out.

ICANN's mission is not the internet, it is the Identifier space. So, if quantum and post-quantum cryptography become an issue for the Identifier technologies or the deployment thereof, then we will be training up and we will be out there, like we do with DNSSEC and other things, actually doing education.

Most of the interesting quantum networking stuff is actually happening in universities at the moment. So, if you've got an education network, those are probably the guys that are leading at the moment. And if you really want to talk, find somebody who likes to geek out about quantum, go talk to the chairman of our board, because she came from a university where they were doing a lot of quantum networking.

So, it's kind of out there in the research. It's coming. There is no doubt it's coming. But is it 10 years from now? Is it 20 years from now? Those are very different planning horizons. It's not next year.

SIRANUSH VARDANYAN Thank you. We have a question from Shanelle. Please.

SHANNELE MCPHERSON Hi, everyone. Good morning. My name is Shanelle McPherson. I am an ICANN84 fellow. Well, alumni, but still fellow now. My question is, how can the technical community merge and coincide with policy make-ups to ensure that we are collaborative with our efforts? I mean, I know, John, you're going to be speaking from an ICANN perspective, but I still think that your advice here can help other technical stakeholders. I mean, policies, they change ever so often. So, I mean, do we need to get our own advisory committees? I'm not sure. But I know that your advice here can help us with our collaboration with the policy makers. Thank you.

JOHN CRANE So, I'm not going to say this from an ICANN perspective, because I'm a technologist first, and the IETF, where I come from, RIPE NCC and the IANA, they all predate ICANN. This is not a new issue. So, I think on Sunday, which I think is tomorrow, because I think today is Saturday, but I'm not sure, the IETF leadership are going to do an open discussion with the ICANN Board, right?

So, we spend a lot of time, my group, we talk about translating. So, we are a translation service between geek and human. Not that we're not humans, but, normal people, should I say. And we do that both ways, right? So, when we're involved in the IETF or we're

involved with an RIR or something, and they have great people, too, that know how to do this. The problem is that in this world, so if you're looking for a career advice, there is a limited number of people that can speak both technology and policy and know how to bridge the two.

So if you can master that, you can have my job, and then I won't have to do it, right? But it's hard. And yes, technologists do need to get involved, but when you talk to a coder who has no interest in policy or doesn't understand how policy affects them, you're not going to get them to come to an ICANN meeting, right? You're not going to get them involved in policy. So, you need to find those people that intersect.

I mean, Merida is a great example. If somebody does policy, it's local policy for technologists, right? Technologists don't actually hate process and policy. We just pretend to, and most of us, at least those of us who live in the real world, know we need it in our life to get things done. So, if you're a technologist and just the fact that you're here shows you have some interest in the policy side, try and learn both. Go and listen to a GAC meeting, Government Advisory Committee meeting. Look at what's coming out of WSIS. If you're an engineer, go look at those things.

If you're a policy person, it's a little bit harder to dive into the deep tech, but not all tech is deep. Go read the advisory or the comments that AWS just put out about their outage, right? You're going, oh, what's the policy perspective? Can I understand what the actual

problems were here from an operations technology standpoint? You'll find that if you read a few of those things, they're not as complicated as engineers like to make things sound.

Engineers and lawyers are bred of the same genetic pool. We like to pretend everything is really hard and complex because it's just what we do, but a lot of the technology is not that complex. If you're willing to sit down and read the 101s, read the basics stuff, you don't have to know the details of quantum cryptography to know enough that it's a future policy issue you need to worry about. Same with AI, same with DNSSEC.

So, it starts with us. We need more engineers that have policy interests and are willing to learn about it, and we need more policy people that have an interest in how their technology affects them. And you probably don't need your own advisory group or, but who knows?

SIRANUSH VARDANYAN Thank you. Go ahead, yeah.

ANUPAM GAUTAM So, I am Anupam Gautam for the record. So, I was just curious that given that IANA functions must maintain nearly like 100% uptime and there needs to be like operational reliability, what KPIs usually does IANA track?

MARILIA HIRANO

So many. So we actually have a dashboard on our website that monitors and tracks against. We have service level agreements with all three oversight partner organizations. So, we have annually, we sign a service level agreement with the IETF where all of the KPIs are listed and we have to adhere to it. And one of the things that our team does is report on it monthly.

We have deadlines even to publish the reports on SLA tracking. We also have SLAs with the regional internet registries agreements, and we have it with the domain name side. And that's where you'll the dashboard on the website. So, they're around in the naming side, which on the domain name system side, it's about 60 different SLAs that we're tracking. And we're actually working with them, with the community now to review those service level agreement, the target metrics to see if they're still fit for purpose. That happens every month in the meeting. We do that review with the community.

SIRANUSH VARDANYAN

Thank you. Any last question? Yes, please. Go ahead over there. I don't see.

DIPSY DESAI

Hi, my name is Dipsy. I had a quick question. So, I was wondering if IANA or ICANN plans to have like a dedicated team for research on AI, ML and its effects on DNS. For example, the recent AWS

outage, they had like more than 75% of their production code running on AI and they didn't have a clue when the DNS went down.

JOHN CRANE

This one's an easy one. No. We have people, we have machine learning and AI experts on our staff for our use and for things that intersect directly with the Identifier system. That is ICANN's mission, but how other people build their systems for online content distribution, et cetera, is not within our mission. So, no, we do not intend to build a dedicated team to worry about some other technology that may be problematic, but it's not our problem at this moment.

We have enough problems in our own identified spaces to worry about all the others. Now, I will say that there are other organizations out there asking about how does AI, and I think they mean generative AI, but I'm not sure because they never really quite say. People throw around the word AI like its candy. But there are bodies out there that are asking who is going to regulate this.

I can pretty much tell you it's not ICANN. We are not the regulators for AI and are not suited for that and highly unlikely ever to be. But those are good questions if you're in the policy realm about, well, who is going to do that? One of the things I found, I've been at ICANN for years, a little bit. sort of predating when ICANN existed. I was involved in the early setup. And one of the biggest, trying to

think of a nice word for it, one of the biggest conundrums that we face on an almost daily basis is that nobody runs the internet.

So, people think that because we do Identifiers, and nobody runs the internet, they're like, well, you must be the people who run the internet. So, therefore, you must regulate everything on the internet. And when we say, well, no, actually, we do not run the internet. No, we are not responsible for the code base that everybody's using. We're not responsible for the contents.

Who here has read our bylaws? Not a single lawyer in the room, I guess. So, upfront in our bylaws, ICANN shall not do anything to cause the regulation of content. It's very explicit on the exact words, so lawyers don't quote me. But there is an explicit clause in there that says we shall not cause content to be regulated. We shall not set policy about content.

So, a lot of what people come to us about is actually the content on the Internet, not us. We are here to ensure that the Identifier systems remain secure, stable, and resilient, and to set policy around certain elements of those. For example, domain name registration. Most of the policy around Identifiers, as Marilia said, comes from the Internet Engineering Task Force or other places, not from us.

So, it's always something where it feels like the right thing to ask is, well, why isn't ICANN doing this, or why isn't ICANN doing that? And it's mostly because of a void in the policy space for many of the

things that are on the internet, but just not us. We don't have the skill set, we don't have the mandate.

SIRANUSH VARDANYAN John, Marilia, thank you very much. Thank you for this interesting interactive session. You now go for lunch and then we'll meet for our next session, How Policy Works. And the session will be here in this same room. Thank you. And with that, the session is adjourned. Thank you very much.

[END OF TRANSCRIPTION]