ICANN85 Mumbai | CF – RSSAC-SSAC Community Open Mic
Wednesday, March 11, 2026 – 9:00 to 10:00 IST

KATHY SCHNITT

Hello and welcome to the RSSAC-SSAC Community Open Mic. My name is Kathy and I'm the Participation Manager for this session. Please be advised that this session is being recorded and is governed by the ICANN Community Participant Code of Conduct, the ICANN Expected Standards of Behavior, and the ICANN Community Anti-Harassment Policy.

This session is designed for community engagement. To ensure we hear from everyone, remote participants, please join the speaking queue by using the raise hand feature in Zoom. In-person participants, you may raise your hand in Zoom. We also will have a roaming microphone available. Please raise your hand in the room and a staff member will bring the mic to you. Before speaking, please state your name and an affiliation for the record. While you are welcome to use the zoom chat for discussion, please note that comments or questions posted in the chat will not be read aloud. All former input should be shared via the speaking queue.

I am now happy to hand the floor over to Ram Mohan.

RAM MOHAN

When you said the roaming microphone, I thought it was going to roam by itself and then you disabused me of that. Before we get started, may I invite our friends who are sitting behind me to come

join us at the You will then not need the roaming mic. You can roam to the mic yourself.

Okay. Good morning here in Mumbai. We are glad to do the Jeff and Ram gig again. It's always good to be able to share what we're doing in both the SSAC and the RSSAC, the two committees that have an explicitly technical mission associated with them. So without further ado, let's just quickly give you an introduction to the SSAC and then I'll hand it over to Jeff to do the same for the RSSAC.

Next slide, please. You can go to the next slide. And the next. Okay, great. So, ICANN's mission is to ensure the stable and secure operation of the Internet's unique identifier systems. That is the core mission of ICANN. And when the Security and Stability Advisory Committee was formed right after the events of 9-11, we spent a little bit of time thinking through what the SSAC's role should be. And our role is to advise the ICANN community as well as the Board on matters that relate to the security and integrity of the Internet's naming and address allocation system. So, our role is tied very tightly, very closely to ICANN's core mission.

So, what are our responsibilities? We engage with the technical community. We analyze risks and trends. We coordinate with various entities that are involved in the naming and address allocation systems. And then we inform the ICANN Board as well as the community on both our observations and our activities. And we provide advice to the ICANN community as well as the Board.

And our recommendations are grounded in security assessments and operational insights.

We're a committee that is not part of the empowered community here inside of ICANN. That means that we are independent in some ways. And it also means that we don't get to vote. And that confers a special standing on us because the weight of our advice and the ability to persuade the community to move in the way we believe is appropriate has to be based on the merit of what we bring in front of the community. We can't just say, we have a vote and we're going to push it a certain way.

So, who we are. We're a diverse group. We're spread from around the world. We kind of the place where we've been growing has been in Africa and the Asia Pacific region. Tara here is to my right. She is the vice chair of the SSAC. And she has been helping spearhead the growth of our membership and the growth and the diversity of our membership. She heads the committee for the SSAC. So if you have an interest in becoming a member, talk to her and she'll be able to tell you what the process is and how you can get moving in that direction.

Next slide, please. So, this is the leadership team. Our term ends this year. I have Tara, Jim Galvin is here in the room. Jim is the liaison to the ICANN Board from the SSAC. Jeff Bedser, as well as Barry. Barry is right here, so is Jeff. These are from the member's side.

And then from the ICANN policy team, we have Carlos and Danielle and Kathy, Dan and Michael. And with that mighty team, the SSAC works on all of the areas. There's a good skill set that comes that allows us to go leverage the skill set to help the committee work and run.

So, the SSAC really focuses on five keystone topics. These are topics where the SSAC believes it has not only a vested interest, but a continuing interest in studying, in analyzing, and in providing advice, recommendations, observations. And those are DNS Abuse, New gTLDs, DNSSEC, Alternative Namespaces, And Internet Governance and The Security, Stability, Resilience Aspects of Internet Governance. So, those are the five core areas that the SSAC is consistently focused on.

Over the years, the SSAC has now been in existence since 2001. So, we're at our 25th year this year. We've done quite a bit of work, and listed here on the screen are significant publications that we have put out. A lot of our work is in DNS security, in DNS management, registration data. But we've also provided commentary and reports on internationalized domain names, on routing security, Open-Source software, things like that.

So most recently, in the last 12 months or so, the SSAC has, on the left-hand side of the screen, you will see our recent publications. We most recently published a report on free and Open-Source software and the software dependencies that are linked to Open-

Source software. Before that, we've also opined on the functional model for Root Server System governance.

Then we've been, for many years now, a steady voice on helping ensure that New gTLDs, as they get introduced into the root, that there is a stable path and there's a secure path for it. Name collisions are a factor. So, we've been providing advice in that area. And we've also provided, we've had a long enduring interest in domain name registration data, its accuracy, and all of the commentary, all of the discussions that happen in this community.

Our focus and the information we provided has generally been more in the technical area than in the policy area. Currently, we're working on several specific areas of work. One of them is, how do you responsibly integrate evolving and new namespaces into the DNS ecosystem? Is there a framework? Are there rules? What should be done to do that? And of course, this is SSAC, so you need a good acronym so that results in RIDE. So, that's the RIDE Work Party. Rick is here. He is the chair of the RIDE Work Party.

We're also, quite a bit of work has gone into the second Work Party DNSSEC operational considerations. And that's the SSAC's look at deployment of DNSSEC. And it's intended to not be just a cheerleading report. It's intended to speak to, if you choose to deploy DNSSEC, what are some of the operational factors you ought to consider? What are some success stories? And what are some problems that have happened? So, that's a Work Party that we're also running. I'm one of the co-chairs of that Work Party.

We have a Work Party on DNS Abuse and AI. We're focusing on what has the advent of AI, what has the impact of it been on DNS Abuse? That is just getting started. And here at this ICANN meeting, a couple of days ago, we had a Work Party meeting where we were looking at what the scope of that Work Party should be. So, that work has begun.

We have another Work Party that has just begun on a topic that we're calling DNS transparency. And the idea there is we have researchers who see that there is an abuse vector that is enabled by the fact that ICANN publishes zone files only once every 24 hours. So, we have criminals who are registering names and using them for malicious purposes and deleting them within the 24-hour cycle.

So effectively, those names never ever show up in the “official record”, but they're causing harm. So, we're calling it DNS transparency, and that's kind of a nod to certificate transparency. So, there's some work there.

And we are, for the -- I think it's the first time, or at least first time in recent memory, we're actively participating in the GNSO's policy development process on associated domain checks. This is an area that is very close to the SSAC’s interest areas because associated domains are causing real and serious damage, real and serious harm on the internet today. And we strongly believe that ICANN ought to take swift and decisive measures to identify associated domain names that are also malicious and then take strong actions

for them. So, we're very keen on that PDP process moving with due haste.

And finally, for the first time in our history, we're starting an experiment. We have an SSAC research apprentice. This is somebody who is, relatively speaking, young in their career, and they are going to be attached to the SSAC work on our Work Parties for the duration of this year. And the SSAC has an annual workshop, and our apprentice gets an opportunity to present at that workshop their findings and their observations. So, they have kind of an end of the apprentice project, if you will, a presentation.

Gustavo is our apprentice, and I see, Gustavo, I think you're online, so welcome to that. So, that's a good sense of what the SSAC is doing.

Next slide, please. That takes us to an idea of what the SSAC is and where we're going. At the end of this year, our terms expire, and we'll keep you informed as to who the next set of leaders of the SSAC are going to be. Thank you. Over to you, Jeff.

JEFF OSBORN

Thanks, Ram. My name is Jeff Osborne. I'm the Chair of the RSSAC, the Root Server System Advisory Committee.

What is the RSSAC? We have a remarkably narrow remit. The Root Server System is made up by a series of operators whose responsibilities are operational. So, policymaking, as much fun as it is for the rest of ICANN, is really not our kettle of fish. The role of

the Root Server System is to advise the ICANN community and the Board on matters of operation, administration, security, and integrity of the Internet's Root Server System, period. It's a really remarkably narrow remit. Thank the because I think Ram and his team are having an increasingly broad one, and so we're pretty thankful we have what we have.

The RSSAC is basically a committee that produces advice, mostly to the Board, but to other ICANN bodies, and we're represented by the 12 operators with a single primary representative and an alternative, and then we have liaisons that are coming from other bodies and outgoing to other bodies.

So, we interconnect with everything from the IETF to the ICANN Board. We have a total of about 28 members in total, and we don't have a nifty slide like SSAC does that shows you all their faces and names, so I'm feeling kind of put out about that and wondering how to introduce those of us who are here. We'll figure it out later.

In addition to the RSSAC, there's a broader organization of experts called the RSSAC Caucus. This is a group of volunteers, and the slide here says it's 128. I thought it was 115. It's a bunch of people who are DNS experts, and just to be very clear, while we're big believers in an inclusive big tent, the RSSAC Caucus is a group of experts rather than a learning environment.

We have a mailing list only membership, which you can come in and join and follow along, but primarily membership is by application of the applicant, and the warning we set is you pretty

much need to have done a large-scale DNS implication on either a large university or corporate or national level. The bar is high, I'll admit. We have people who come back and make the argument that they're better than we think they are, but this is intended to be a group of experts that does much of the work that we do in producing documents and doing research. It keeps us transparent. It keeps the framework broad, and it's an interesting way to do work.

Like everyone else, we put out publications. You can find them on the ICANN website if you're interested enough to do a deep dive into RSSAC. You could get most of the way there with the documents here. I'd recommend if you wanted to start, the RSSAC001 is the history of the organization. It's all of 47 pages. I know of nobody outside of ICANN or the technical community who has ever read the whole 47 pages, but you could give it a try.

Recent publications we did include things like changing IP addresses of root servers, which is remarkably complicated. Things in the root server world tend to last for very long periods of time, and we don't make changes like that lightly. We've recently reported on incident reporting. We did a report on the governance group, which is separate from RSSAC.

Yesterday was the first public airing of the governance working group's governance structure, and there was remarkably little discussion about it then. It might come up at the public forum. I'll refer any questions about governance of the Root Server System to

the GWG. There are several members of it here. I'm not personally a member.

Stuff we like to talk about includes the service expectations, measuring, metrics. We love numbers. We are extremely, whatever the polite way to say geeky is, we're a bunch of nerds who keep a thing running and are very proud of a system that operates trillions of times a day and has worked without a blackout for about 37 years.

Our other favorite topic is anything about the DNS root system because that's what we like to talk about. Next slide, and I think that might be the last. Well, I'm the chair, as I said, and Hans-Peter Holen, who couldn't be here. Hans-Peter, are you online?

In my day job, I'm the President of the Internet Systems Consortium, which is the producer of BIND 9, which is one of the leading DNS name server pieces of software out there. It's Open Source. We're a non-profit. It's given away for free. We do all this stuff for free. We operate a root server for free. We give away the software. There's no money in any of this.

Hans-Peter has a lot more depth than I do as the President of the RIPE NCC. He has experience in everything from running an RIR to running a root server operator to all the rest of it.

BARRY LEIBA Yeah, because I see you side by side there with your previous picture. Grow your beard back. Come on.

JEFF OSBORN

Barry, let me give you my wife's email address. I grow a beard, and then it gets to the point, and she sits there and just goes, with the beard, huh? Then I give in because I'm that guy. I'm going to tell her, Barry insists I get a beard back. Thank you very much.

Good. Next slide. That might be it. That's it. Thanks for your time. For both of us, I guess, are there any questions?

RAM MOHAN

Before we open the queue for questions, ICANN Org wants to clarify something brought up during the SSAC Lightning Talk session yesterday. So, we have Francisco here for that. Welcome.

FRANCISCO ARIAS

Thank you, Ram. Hello, everyone. This will be quick. Just wanted to, as Ram said, clarify something about yesterday during the SSAC Lightning Talk presentation on wildcards and brand TLDs. It was mentioned that ICANN generally seems supportive of the use of DNS wildcards on TLDs. Unfortunately, there was no time for me to clarify that. So, I wanted to clarify that ICANN Org maintains a clear and unambiguous approach regarding wildcards. ICANN Org is required to implement the direction from the ICANN Board and provisions in the registry agreements.

The ICANN Board of directors addressed this matter in a resolution in 2009, prohibiting DNS redirection and synthesis, including wildcard records at the top level for TLDs. And as a consequence,

the Base Registry Agreement prohibits synthesizing DNS resource records or using redirection within the DNS, including DNS wildcards resource records. So, just that. Thank you.

RAM MOHAN Thank you, Francisco. Rick?

RICK WILHELM Thank you, Francisco, for that clarification.

RAM MOHAN Okay. Now let's go to any questions in the room or online. Kathy or Dan, the protocol is you raise your hand in the zoom room. Okay. As Jeff and I know, usually this is the most awkward part of our meeting because somebody has questions, but they haven't mustered up the wherewithal to ask it.

JEFF OSBORN I will be your plant then. Something that has come up this week, and Tara and I were just talking about it before you showed up, the RSSAC and the Board met the other day and they asked the question they always ask which is effectively what keeps you up at night. And we're kind of proud that the root service system is so solid. It isn't anything technical. It's something else.

The last time they asked, I said, it's tuition because I got a kid in school. This time they asked it slightly differently. And they said, what would you like us to be certainly aware of when we look our

five-year Strategic Plan? And I said, well, God, AI, you can't possibly be right in the fifth year of your plan about what the unintended consequences of AI are. And so, it becomes interesting.

So, then somebody has come up with adding an AI question to an RSSAC work party, and we kind of went, I don't think that's us. And I thought, oh my God, is the SSAC going to get stuck with this? So, I'm just wondering if in advance, have you been thinking about, somebody's going to end up saying who at ICANN deals with the two varieties, the technical, oh hell, something broke, and the strategic, what are we going to do about these aspects of AI?

RAM MOHAN

Great question. And this is to address some of this is why we have started up this work party on DNS. I mean, DNS Abuse in AI. So it's been… it's kind of narrowly scoped. So, it's a little bit more narrowly scoped to DNS Abuse in AI rather than the DNS in AI, so to speak. But in our informal discussions inside the SSAC, I would, the way I would characterize it, Jeff, is that we're not seeing, at least on the attacker side, necessarily new techniques.

But what we're seeing is a significant increase in both the scale and the speed of the attacks, and kind of the complexity of the attacks are getting more and more sophisticated because the engines are able to learn from their prior iteration, right? So, that's been the general thrust of our discussions inside. Barry?

BARRY LEIBA

This is Barry Leiba from SSAC. Divide the issues of AI with respect to security into three pieces. There's using AI to abuse, there's using AI to detect abuse and mitigate it, and there's, well, I guess that's it, attack and mitigation being separate.

On the attack side, the general issue is that we're not seeing yet anything that's different about the attacks, but the AI makes them scale in ways that we could not imagine before. For instance, we can now do targeted phishing attacks on you rather than it being Kurtis or somebody who's running a large organization or something. And that's scary.

And when that starts being used to attack the DNS, we're going to have to do a lot of thinking about how to deal with it. But the attacks themselves are known. So, then we have to watch for what happens when we see attacks that were hitherto unknown and we never thought about that. And it would be nice if we could back up, use AI to predict what kind of attacks AI will be able to make.

And we're seeing that in the AI engines are now doing better than humans by far in finding bugs and finding exposures and vulnerabilities in systems. So, I think that may be some avenue that SSAC can investigate and how we can use AI to proactively look for vulnerabilities in this area.

RAM MOHAN

Maarten?

MAARTEN BOTTERMAN Yes, thanks. And yeah, I understand the issue and I heard Jeff say yet. And of course, the thing is the skill that may be a new challenge, even if the threats are similar.

BARRY LEIBA As I said on the microphone the other day, whatever AI isn't doing yet, it will.

MAARTEN BOTTERMAN Yeah. The other point I wanted to bring forward, because I've asked a few people, so what about quantum computing and how do you deal with it? And most people are not worried about it yet because it's still far away.

At the same time, what we know if the quantum becomes a threat, as well as an opportunity, this will go with new requirements to the hardware as well and things like that. If you look back to IPv6 introduction, it took a while before the system, after IPv6 was recognized as important, that the whole system was ready to deal with the larger keys.

And now for quantum computing, we'll see a similar hardware challenge as well, which means that the lead time to prepare for it will be longer than for AI, which is similar but skills differently. So, I would ask how you see at what point you think we should pre-think quantum computing and the effects and what we need to do.

I'm pointing out there is a session this afternoon that at least touches upon it a little bit with quarter past one, I think, one of the DNS sessions.

RAM MOHAN

Thanks, Maarten. We've had several discussions inside the SSAC on quantum computing and the advances and the potential impact. There are two points I'd like to make.

One is the recognition that if you look at what is the threat and what is the landscape, we think that there's not a whole lot of secrets that are held that necessarily get exposed because you have algorithms that can be very easily cracked. So, if you look at it from a pure security point of view, those who have credentials at stake and protecting credentials using cryptographic methods have a pretty high urgency associated with it. It doesn't mean that we don't have it. It's an important issue, but we're looking at it and saying we can probably see a little longer runway for that compared to AI because AI and the changes that are happening from AI, they're happening now and they're happening rapidly.

Now, yesterday in our session with the Board, Tripti, the Board Chair, who is also in her day job deeply involved in the quantum areas, was saying that the advances in the technology for quantum, it's going faster than had earlier been anticipated.

So, it's an area that has to be looked at. We don't have a work party or kind of specific focus inside of the SSAC as of yet, but I mean,

relatively speaking, I would characterize it as it's more a background area that we're watching rather than a foreground area we're working on. Peter?

PETER THOMASSEN

Yeah, Peter Thomassen, SSAC. So, for some extra context, the quantum threat is pretty well understood. It is pretty well understood what sort of algorithms can run on a quantum computer if a large one would be built and in what ways that would threaten which sort of security properties of what kind of classical algorithm. That's a little different, I guess, from AI because there it's sometimes quite unclear what can happen in the future.

So, for quantum computers, the threat is sort of well-defined and also depending on which security properties you concern yourself with, the urgency varies vastly. So, for example, if you have an HTTPS connection today that contains, I don't know, a sensitive email, somebody might record that today and then use a quantum computer in 10 years to retroactively read that.

So maybe the email today should be protected with something that already protects against that. But that is not something that the DNS deals with because the DNS is public, so there's no store now decrypt later problem. The security problem in the DNS is more about signatures and signatures are only attackable at the time when they are used and that is usually shortly after they are generated, like a few days or weeks or something or seconds.

And so, the problem isn't as urgent there. Nevertheless, the problem has been recognized and the IETF has an informal group that meets at every IETF meeting that is called PQ, Post-Quantum DNS Excite Meeting, and new research is presented about how that's developing and how the DNS could be improved to include such new resilient mechanisms.

And so, it's on the agenda. It's not extremely urgent. It is also a tricky problem, but people are thinking of it and I'd say it's in the right state for the situation we're in.

JOHN LEVINE Yes, while agreeing with everything that Peter says. I mean, in practice, what this means is that DNSSEC will have a new key algorithm, so people will program the new algorithms into their signers and resolvers and we'll need to do a key role from some of the current keys to new key algorithms.

Fortunately, we've already done key roles to new key algorithms, so basically everything ICANN needs to do is executing a process we already understand. So, it's simply a matter of waiting for the underlying software to catch up with it, then we can just do it.

MAARTEN BOTTERMAN Yes, thank you for that and it's all in the room now. I'm not a tech expert. I'm more a strategic expert. And the thing is, what is the effect in terms of the number of characters that we need to use and the length of the scripts? And will the infrastructure be able to deal

with this? And infrastructure investments take a lot of time to roll over.

With IPv6, it wasn't a problem because we could gradually move over. With this, once really the shit hits the fan, we don't have time. So, we need to preempt that. That was my only thought from a strategic perspective. If you comfort me and say, oh, no problem.

JOHN LEVINE: I've got about two-thirds comfort you. For SSL certificates, they indeed are getting much bigger and you may have seen a bunch of press releases that Google has come up with a clever way to do the miracle trees of hashes of signatures. Since there's a hard limit of 64k for a DNS packet, people are thinking very hard about how do you make things fit? So, we're going to do some kind of hashing to keep stuff to a reasonable size. Basically, the signatures can't grow too much and still fit. So, we'll figure out some way to make them fit and it'll be fine.

RAMMOHAN: All right. Jim.

JAMES GALVIN: So, yesterday in the last Board bilaterals at the NCSG, Tripti asked this question and she asked, is AI a verb? She says, I'm pretty sure we've been AI'd the last couple of days. Because it is true that AI came up in every single Board bilateral. I mean, it's just the

discussion in the community. And I think all of that is a good thing. So, it has not escaped attention or radar.

I also just wanted to say, as a happy coincidence, I suppose, it certainly was not planned. But as part of the annual strategic review, and for those who are paying attention, that's been a community topic and going on out there. The Board actually had its annual strategic review, a workshop session over the weekend as part of its workshop.

And it is interesting that AI obviously came up as one of the disruptive technologies that, as we look forward and think about what do we have to concern ourselves with and what is likely or not likely to impact ICANN, it certainly hit the list. And the top of the list, in fact. And post-quantum computing also got on the list. But it was recognized for all of the reasons and discussions that we've had here that there's probably something there.

We do have to worry about the route and the signing there. But other than that, it's not of as great a significance as AI is. So, there is interest in the Board on trying to look at the impact of AI and where it goes and what happens. And I am hopeful that as a result of SSAC's bilateral and the resiliency plenary that we had, that it will be on the list of things that will be explored more directly, and that SSAC will have an opportunity to contribute to all of that.

So, we'll see. It's important to keep talking about it and raising awareness everywhere, not just here. So, thank you.

RAM MOHAN Thanks, Jim. Bruce.

BRUCE TONKIN Thanks, Ram. I'm interested from an RSSAC point of view, I guess, is do you do much in the way of cybersecurity exercises or simulations? And for example, let's assume the U.S was completely uncontactable for weeks by the rest of the planet. What would that do? How would you, because the DNS signatures and stuff would start to expire, but just different scenarios like that?

JEFF OSBORN That's a hell of a scenario. Somebody with a more technical background want to give this a try? I'm looking at Liman and he's --

BRUCE TONKIN I'm not so much wanting to go into the actual scenario, but more that you are doing scenario planning and exercises.

KEN RENARD This is Ken. That particular scenario involves a lot of things that are outside of RSSAC, like the IANA and how they would publish the zone. There are technologies that can help us here, like Local Root, but the Root Server Operators are purposefully independent, autonomous, so we do our own exercises. Outside of the ICANN environment, we do coordinate and talk shop and think about

these scenarios and collaborate. But the bigger scenarios, like you discussed, really involve beyond just RSSAC into the IANA world. So, fair point.

BRUCE TONKIN

And that would be exactly my point, because big disaster scenarios are out of your control, which is why you sort of want to do scenarios and actually think about how you would actually respond to each other.

JEFF OSBORN

I think an important point to make, at the risk of sounding self-serving, is a lot of the normal issues about, oh no, you had an outage, what does that mean, can affect the Root Server System very, very differently, where we are providing the address to 1,450 TLDs.

So we get that from the IANA, cryptographically signed by the RCM, and my first thought was, oh hell, they're in California and I have no idea, because all I do is wait like a good civic servant for this thing to be handed to me and then serve it to the 400 locations around the world that my company runs.

So I think the question is, is Kim here? I mean, the real question is, how does IANA handle that? If you're saying, you know, the internet is bifurcated and North America is an island, what the hell happens to the rest of the world? Well, as we've seen a lot of times, Hans-Petter's organization, Lehman's organization, and Hero's

organization, independently outside of the United States, are more than adequate to provide the root server fulfillment needs of the world by a factor of, I don't know, an order of magnitude or five.

So, the reason you stumped me right there was, what does IANA do? And so that's a really good question for IANA. But again, the reason we have a problem with doing the security scenarios is, if you were not reminded for a week that the country code to call your cousin was plus 44, you'd probably still remember it. I mean, the kind of information that the root zone carries, doesn't really change in dramatic and important ways that often. And it's hard to say this without sounding like, gee, we're not important. But the case is, a 24-hour outage, for instance, of the entire system, you could argue would be almost unnoticeable.

Not to mention unimaginable. Because, I mean, Anycast really, really, really changes the risk profile of all this stuff. You think about banks that operate on a server and a high availability other server, and if one goes down, the other is there. We could lose 95% of the devices out there and nobody'd notice.

It got so shockingly overly resilient and redundant with the introduction of Anycast that it's kind of a hard scenario. I'll repeat the joke that it's not a joke, but the chairman of my Board is a guy named Rick Adams, who started one of the big internet providers back in the 90s and is brilliant and all the rest of it. And I was saying to him, can you imagine a failure scenario for the Root Server System?

And he stopped and he looked up and he said, in the third year of nuclear winter, there is a situation where, and I was like, okay, that's what we keep coming up against. There are so many things to worry about, like food and water and the heat death of the universe, sort of before the reasonable scenarios have us be the weak part of the system.

And again, it comes off sounding really arrogant, but when you look through how the parts work, I have yet to see a really important strategic test that would make sense of what should be worried about that we're already not worried about and we aren't already doing something about. Is that reasonable? And Liman?

LARS-JOHAN LIMAN

Hi, Lars-Johan Liman, RSSAC. Yes, we do conduct exercises and also, at least speaking for Netnod, we have to go through the formal procedures of doing risk analysis and stuff. We need to be, to do that in our case, because we provide commercial DNS services in parallel to the root service and the customers expect that of us paying customers and they will not pay if we cannot live up to that.

So, not only in our case do we conduct such exercises and risk analysis inside Netnod, but we also lead such exercises with other customers. So, to us, it's a very integral part of what we do. And that risk analysis has a very wide pamphlet of things that we need to look at and assess when we do things.

And I'm with Jeff that the technical operation of the servers, that is not something that keeps it up at night. But there are things that are outside our control which could have influence and the supply chain of data is where the border lies. And I honestly think the Root Server Operators and IANA could do a little more in talking about what the potential risks are there. I would support going down that path actually. Thanks.

JEFF OSBORN: And thank you, Liman, for proposing that you will run that work group. I'm looking forward to it. Jim?

JAMES GALVIN: So, I actually appreciate Liman's answer, but I have to say, Jeff, that I actually found your response a little bit dissatisfying in the following way. I have no doubt that all of the individual root server operators are on top of exactly what they have to care about. They're running a critical resource of the internet. They all know it. I'm sure that they all individually do their risk analysis.

They're doing their audits and they're making sure that their operation works. But I think where Liman landed is really kind of the point here. And I think that Bruce asked a very top-level strategic question. The Root Server System is more than just an individual root server operator. It is big parts.

If there's one big takeaway from the resiliency panel that happened yesterday that we had, it's all about dependencies and the complex

dependencies that any complex system has and the things that we don't know. I mean, most of the major disruptions that we've been seeing lately over the last couple of years are because of some little thing that happened that has cascading failures. I mean, it's the supply chain risk, as Liman just got to.

I think in our Root Server System, that's a real issue. There is this player, IANA, and all of the parts of that. And it's an interesting situation that VeriSign kind of serves a dual role there. So, they're part of that distribution supply chain system as well as separately being a root server operator.

And then you've got ICANN and IANA. And you have the distribution of the root zone for those who want to do local root and those kinds of things. And how those pieces fit together and what it means when there's a failure in there. So, I think Bruce's question is really a question he asked specifically about root server operators. But I think that as ICANN, we need to take on board the fact that there is room for examining resilience and what it really means to us, especially in the face of AI. We all accept that AI, as Barry says, is going to do things faster than any human is going to do it. And we're already seeing that.

It's finding bugs and codes and errors and problems all across the Board. And I think it's fair to worry about whether we have deeply examined the Root Server System as a whole, not because any individual operator is a problem, but because of the dependencies

and complexities that are in the system as a whole and in the ecosystem.

So, I mean, I appreciate your comment about root server operators. But I wanted to up-level your response into something a little different and being a little more responsive to what Bruce was asking. Thanks.

JEFF OSBORN

Okay. I'm going to say follow the money. Because what he said was not that his organization does all of these things for the Root Server System. It said he has commercial customers, and that's why he does it. So, the commercial customers who help pay for the millions of dollars my company pays for the benefit of the earth don't exist. Nobody's paying us to do this.

So, this has been one of my issues from the beginning, was if you want to put demands on Open-Source software developers or people who are freely providing a Root Server System, that's nice. Your organization makes money on every domain name that goes through. And everybody who's able to say, I can kick this up a notch, has a place where it comes from. But for some of us, this has literally been something ISC has been doing for decades without failure.

And when somebody walks up to me and says, you're doing a bad job of it, do it better, I think I do a pretty good job of not responding in a bad way.

JAMES GALVIN

Just one last comment from me. I certainly, and I tried to say up front, I mean, I know that the root server operators are all on top of their individual systems. I think the question here is about the root server management ecosystem as a whole. Root server operators are part of that as individuals.

They're all fine. But we are part of a supply chain. And ICANN has a role in that. IANA has a role in that. And that's the part of the system which really does have to be examined and to determine where the gaps are, where the issues are, and where the risks might be. And then we have to have some discussions about what to do about it. That's all.

JEFF OSBORN

A supply chain implies commercial relationships that don't exist. And in economics, there are uncosted externalities that always mess up the theoretical. And I will argue this is one of those cases. And it's the gorilla in the room. And I'm going to keep talking about the gorilla and feeding it bananas. And maybe I'll keep getting ignored. Maybe I won't.

RAM MOHAN

I'm just going to put a two-finger on that, Jeff. I think you're kind of deconstructing it to commercial versus non-commercial. But I think the higher order issue is that there is a critical infrastructure function here. And it's an interlinked function beyond one

operator, regardless of whether that operator is commercial or non-commercial. And I think part of what is the evolution that's happening and part of the resilience issue that I think is upon us is it's not that that part of the system breaks.

It's systems that are based on top of that that have disruptions and have problems. And you end up having governments saying, oh, is there a plan? Were there measures? Was there an exercise? Things like that. So, I think there is a larger level systemic interdependencies piece that has to be looked at beyond an individual Root Server Operator and how that is doing a great job in serving its purpose.

JEFF OSBORN I will continue to not be a fan of unfunded mandates. You know what I should have done before I did this is this is why I have an RSSAC hat, an ISC hat, and a 'Just Jeff's Opinion' hat. So, I should have put on my Just Jeff's Opinion hat before I said that. So, my apology is for those who thought I was in an RSSAC hat.

RAM MOHAN Well, you're here as the RSSAC Chair. So, it's nice that you have the Just Jeff's Opinion hat. But the reality is that this is a question about root servers, et cetera. So, I respect your personal opinion. But I think downstream, we ought to be, maybe not even downstream, maybe at the moment is here, but we ought to be

looking at the fact that those unfunded mandates, there is an opportunity to do it voluntarily now.

I'm worried about that opportunity going away and having authorities come and say, you do it or else. So, that's what I'm worried about, Jeff.

JEFF OSBORN

I should have said the same thing in my ISC hat because it's also true for my ISC hat. As a public benefit company that is doing all of this for the good of the world, it is challenging enough making payroll. And it becomes especially challenging when we get mandates to do difficult and expensive things and we're expected to hold a bake sale.

And there's a part of me that says, gee, this is kind of outside the remit. Let's keep this more friendly. But on the other hand, it's an unspoken thing that doesn't come up often. And I kind of felt like we weren't getting flooded with questions, so it wasn't a horrible time to bring it up. So, I will definitely apologize to you personally and SSAC if it's an inappropriate time to bring it up. But it's an area that I think is under addressed in the Internet Governance world.

RAM MOHAN

Yeah. And I don't know that we're at opposite ends of it, but I think that at least what I'm saying is that the reality in front of us is we may wish to not get unfunded mandates, but the infrastructure that you're all operating to great benefit of humanity is I think

getting a lot more scrutiny from places that we wish it wasn't getting that level of scrutiny. That's all.

Okay. There's a next question here, Francis Ojeifo. Francis, please go ahead.

FRANCIS OJEIFO Good morning, everyone. Thank you. With the trending encryption DNS reshaping global query pattern, how is RSSAC observing the impact on root servers' traffic visibility and what is the operational consideration to maintain resilient without compromising the privacy?

KEN RENARD Thanks for the question. This is Ken. For the most part, the bigger picture with the encrypted DNS protocols, most of that happens between the end user and the resolver. That's the 80, 90, 95%. With that said, there is more and more encryption happening between the resolver and authoritatives. But that first part, it really doesn't change what the Root Server System sees.

The encryption from the client to the resolver doesn't change much. Resolver to authoritative, there are some Root Server Operators that have, I guess we're officially calling it experimental, but have started serving encrypted transports from recursives to the root as an authoritative. And, you know, I would expect some data to be coming out in the next couple of months on traffic volumes and things like that.

We as Root Server Operators have always felt very strongly about the privacy of the data that we see, we use it for to maintain our own systems. We don't share it. We don't share it monetize it in any way. And raising the bar, this is my personal opinion as a Root Server Operator, raising that bar if people are sending us encrypted traffic, we hold an even higher bar now. You know, that's very much private data. So, that's my take.

RAM MOHAN

Any other questions? We are almost at time. Anything in the room? Nothing in the room? Anything online, Dan? Okay, Jeff, closing comments.

JEFF OSBORN

Thank you very much, everybody. And I would really like to stress, Ram, I have a bunch of strongly held opinions. So, do you. I have a tremendous amount of respect for you, the team you lead, and all of the work you've done for the internet at large. And if any of this came across as anything other than respectful, but just my input, I'd just like to apologize for that. Because absolutely not my intention.

On the other hand, if anybody wants to talk about the fascinating externalities that Internet Governance entails, and their economic roots, I'm free all week.

RAM MOHAN: Thanks, Jeff. Look, I mean, we're good friends. We go back a long way. I'm not worried about any of this. And I think it's actually good to have a forum where we have a frank exchange of ideas. And ideas ought to battle each other. And they do the best work when the foundation underneath is one of friendship.

So, no offense taken at all. I think it's actually an important discussion to have. And I'm glad that we're having it. And you've been part of it in many other forums before. So, this is one more forum where it's happening. But I appreciate the question from our community that really sparked the topic. So, that's where it really comes from. And we all are trying to do the right thing in the best way we can. And I think it's always good to have open discussions and see how to uplevel everybody. So, look forward to that.

And with that said, thank you so much. This session is adjourned.

KATHY SCHNITT: Please stop the recording.

[END OF TRANSCRIPTION]