ICANN85 Mumbai | CF – From Stability to Survivability: ICANNs Role in the Future of Internet Resilience
Monday, March 9, 2026 – 10:45 to 12:00 IST

KATHY SCHNITT

Hello, and welcome to From Stability to Survivability, ICANN's Role in the Future of Internet Resilience. My name is Kathy, and I am the participation manager for this session. Please note that this session is being recorded and is governed by the ICANN Community Participant Code of Conduct, the ICANN Expected Standards of Behavior, and the ICANN Community Anti-Harassment Policy.

Interpretation for this session will include English, French, Spanish, Chinese, Arabic, Russian, and Hindi. Please observe the following guidelines to participate in this session. I will also post them in the chat for your reference.

There are three ways to ask questions. If you're here in person, please go to the standing microphone and wait your turn. If you're attending virtually, submit your question through the Q&A pod. I will read that question aloud, or you can raise your hand to speak directly. Simply click the Raise Hand icon at the bottom of your screen to join the queue, and we will unmute you when it's your turn.

Whether you are in person or remote, when it is time to speak, please state your name for the record, the language you will speak if speaking a language other than English, and speak clearly and at a moderate pace. I will now hand the floor over to Ram Mohan.

RAM MOHAN

Thank you. Namaste, and welcome to this plenary. My name is Ram Mohan, and I'm the Chair of the ICANN Security and Stability Advisory Committee.

Looking out on the streets of Mumbai, you see a master class in resilience. This is a city that never stops moving, not because every light is green, but because it has an incredible capacity to route around obstacles. The internet is no different. But today, internet resilience is no longer a question of whether the packets reach their destination. It's a question of whether the system of trust that moves these packets can survive the many storms currently gathering at its borders.

This isn't just a tech story. It's a story about hidden dependencies, power, cloud vendors, global regulations that we rely on but do not control. And as we move toward a world driven by AI and constant connectivity, understanding these vulnerabilities is the difference between a minor inconvenience and a global shutdown.

Resilience is the ability to maintain a single source of truth even when the world feels fragmented. Today, we are not here to discuss politics. We're here to discuss the technical Nexus, the protocols, the infrastructure, and the operational stability that keep the global route anchored while the winds of change blow.

We're talking about whether the systems that billions of people rely on every day for communication, commerce, public services, and

security continue to function in the face of technical failure, geopolitical tension, and increasingly sophisticated attacks.

So I have here with me a distinguished panel and before we get to the panel, I want to share with the audience we plan to use Mentimeter for audience engagement throughout the session. And what you'll see up on the screen is a QR code. And when you see the QR code, grab your phone and scan that QR code and you will see some questions.

We would love to get your perspective on those questions and we will provide the input that you're providing to us. We will share that with you as we move forward. Fiona and I are joined by five panelists. Danny McPherson, he leads VeriSign's technology and security organizations. Danny has actively participated in internet operations, research, and standardization since the early 1990s, including serving on the Internet Architecture Board and chairing an array of Internet Engineering Task Force and other working groups and committees. He has authored several books and numerous patents, Internet Protocol Standards and Network and Security Research Publications.

We're also joined by Bruce Tonkin, who is the Chief Executive Officer of the .AU Domain Administration, AUDA. Bruce has been there since 2017. Prior to that, he spent 18 years at Melbourne IT, which was one of the first five ICANN registrars. He also spent nine and a half years on the ICANN Board from 2007 to 2016, and he was the chair of the DNSO slash GNSO for five years prior to that.

We're also joined by Mr. M. A. K. P. Singh. Mr. Singh currently serves as the Chief Technology Officer at CyberPeace and is a former member and Chief Information Security Officer at the Ministry of Power at the Government of India. In that role, Mr. Singh led key initiatives in energy transition and cybersecurity until he retired. He has over three decades of experience in India's power sector, guiding the shift toward non-fossil energy sources, such as solar, wind, and hydro.

We're also joined by Dan York. Dan is the Senior Director, Online Trust and Safety at the Internet Society, where he leads the development of the Internet Society's online trust and safety hub. And he participates in technical communities, including the IETF. And here at ICANN, Dan has been a member of the Program Committee for the ICANN DNSSEC and Security Workshop since 2014.

He has been online since the 1980s and is the author of multiple books on networking, security, IPv6, and Linux. As a staff member of the Internet Society since 2011, he has worked across a broad range of initiatives, including internet resilience, internet shutdowns, DNS security, IPv6, and low earth orbit satellites.

And finally, on our panel, we also have Paul Vixie. Paul Vixie designed, implemented, and deployed several domain name system protocol extensions and applications that are used throughout the internet today, including dynamic updates, network reputation, and the BIND Open-Source software. He is a

former SSAC member, and he currently serves on the RSSAC. Fiona, do you want to take a moment to introduce yourself as well?

FIONA ALEXANDER Sure, hi, everyone. Fiona Alexander with Salt Point Strategies, but a long-time participant in ICANN in many hats from years past. So happy to be joining you from Washington DC.

RAM MOHAN Thank you. So, the internet's original foundations, DNS, IPv4, BGP, still keep billions of people online, but the environment that all of these protocols work in is entirely transformed. We observe, with increasing frequency, severe and widespread cascading internet disruptions that are caused by failures in critical external systems the internet relies on, systems such as power grids, cloud platforms, and complex software supply chains.

The problem is not protocol fragility. The problem seems to be environmental fragility. We are at an inflection point. The focus for today is not a tutorial on how the internet works. We're not also here to debate ICANN's bylaws or ICANN's mandate, but we're here to discuss what happens when core systems around the internet break, and what happens when user applications on top of these core systems break. Fiona.

FIONA ALEXANDER Hi, thanks, Ram. So, I think we wanted to provide a little bit of context for the conversation for today. And several of us, including

Ram and Dan and Danny and others have been involved over the last year and a half in an effort by the Marconi Society looking at internet resiliency.

They have established Internet Resiliency Advisory Council which several of us were on. And then they also had a series of meetings and workshops where they looked at a set of issues and tried to figure out what should we do and how should we make internet resiliency kind of a core issue set going forward.

So, in November, 2025, they held a workshop and a forum. These meetings represented the culmination of a yearlong collaborative effort to address critical vulnerabilities and global internet infrastructure. Building upon an initial gathering at the National Academies of Sciences here in Washington, DC and sustained work online through two dedicated working groups.

One, the Internet Resiliency Supply Chain Mapping Working Group that I was involved in. And second, the Hyperscaler Engagement one that Ram was very involved in. Both working groups put together a series of reports and both meetings united operational, technical, policy and governance leaders to translate diverse expertise into actionable resilience strategies.

The core takeaway from this effort is that resilience must be treated as a foundational design principle, not a secondary consideration. So, if we look at the themes of the Marconi Society Report and we look at the sort of the themes that came out from ICANN's Security Stability Advisory Committee and SAC132, which came out in

September, 2025, which looks at how the DNS depends on free and Open-Source software. We have four specific themes that we want today's session to cover.

The first, major power grid failures and what that means for the internet, cascading outages from cloud and API failures, policy and regulatory interventions that can have DNS implications, whether they're unintended or intentional and software supply chain attacks at unprecedented scale.

So, with that context, we want to go ahead and give each of our panelists three minutes to make their opening intervention. And if we could ask the panelists to speak, please keep to the three minutes, that'd be great. So, we're going to kick off with Danny. Danny, over to you.

DANNY MCPHERSON

All right. Thanks, Fiona, for that and greetings everyone. I'm going to focus on core internet infrastructure, but these comments apply equally to all the systemic threat areas Fiona outlined.

The core protocols that enable the internet, the border gateway protocol for inter-domain routing and the domain name system that effectively enables global navigation scale extremely well, have proven to be extremely robust in the face of instability. However, these protocols were not originally designed with security in mind, but rather relied on implicit trust among a relatively small community of operators.

Now, as we all know, the world has changed and the community of operators has greatly expanded and these core internet protocols and their supporting infrastructure have been and continue to be retrofitted with security enhancements.

Some examples include resource PKI for enabling a more secure inter-domain routing system and DNSSEC for data origin authentication and integrity protections. While these are all important advances, they also expand the operational surface area that must remain reliable. Simply put, each new security enhancement adds complexity and with complexity comes additional failure modes or ways for things to break.

In some ways we've created a resilience paradox. The mechanisms designed to protect the internet can themselves introduce new systemic dependencies and problems. However, these security enhancements are aimed to prevent even more malicious catastrophic disruptions and require careful deliberation and extreme rigor in implementation and operations.

With foundational protocols that underpin critical systems, you want to minimize systemic dependencies and avoid circular dependencies, but sometimes these are unnecessary. Furthermore, when you take inherently decentralized protocols and add new systemic dependencies, even when loosely coupled, it becomes critical to design buffers and operational guardrails of multiple layers of the system so that the system holistically can

absorb unexpected shocks rather than propagating or cascading them systematically.

When thinking about shared fate and stability, I think about what do I ultimately care about? Where does it live? What enables it? And what are the performances security controls required to operate and protect it? And what are the risks that need to be mitigated associated with it? Or more simply put, what do I ultimately depend on--?

KATHY SCHNITT: Danny, sorry to interrupt. Can you please slow down a bit for the interpreters?

DANNY MCPHERSON: Yeah, sorry. Excuse me. Yeah, no problem. And what depends on me? So, for DNS infrastructure operations, those things include underlying transport substrate, the various components of the routing system, which now includes RPKI, network and computer hardware, and OS diversity, service application diversity, systems resilience and agility, and the supporting identity and access and control systems and network and security endpoint controls.

As infrastructure becomes more interconnected and increasingly concentrated in large multi-tenant environments, the potential blast radius also grows. A monoculture of practices within hypergiants or hyperscalers or CDNs and transitive trust

dependencies in software, transitive trust in network and security protocols, et cetera, all impact that robustness calculus.

It's critical that operators enumerate these and understand their attack surface and that both impact and consequence analysis of various failure scenarios are properly considered and remediated where appropriate, ideally before failures occur. That's it. My opening statement.

FIONA ALEXANDER: Thanks, Danny. Our next speaker is Paul Vixie. Paul, I think you're there, right on screen.

PAUL VIXIE: Hello. Can you hear me?

FIONA ALEXANDER: Yes, go ahead.

RAM MOHAN: You're a little faint, Paul, so perhaps a little closer to the microphone.

PAUL VIXIE: All right. I'll do what I can. I'm going to turn off my video now. So I want to talk a little bit about the software supply chain, which is always topical. The internet could only have been created through a whole bunch of non-contracted dependencies. In other words,

software and protocols were being created everywhere by a lot of people who were interested in seeing things work.

And there's not usually consideration paid if you were developing software and putting it up on the internet for other people to fetch and download. You weren't expecting to get paid for that. Your motivation was something else. And what that meant was this business of non-contracted dependencies has remained to the current day.

I think all of us understand that software has bugs, that all software ever has had bugs, and that we expect that all software forever will have bugs. It is unnerving to download software, whether Open-Source or maybe an app for your phone, whatever it may be, knowing therefore that it has bugs, but that you don't know what they are yet. But the patches are coming. I believe any one of us has a constellation of laptop, smartphone, whatever.

We're expecting to see about a gigabyte a week in software updates coming toward those devices, and that is mostly to fix defects. Now, this is not scaling, although we could only have gotten here that way. It's plain to all of us who think about these things and talk about them that we're going to have to find something better because at scale, what is happening is that a software creator will understand a new defect in their work and they will fix it.

And then they have to wonder, is this security related? Is it something that if I publish it, that a lot of people will be injured by other people, attackers who will use it before it can be patched?

And if so, how do I get the patch out there before the attackers can get their hands on it? This is a huge problem. And you'd like to maybe tell these people, libertarianism has a long hold on internet culture, and you might just say, just publish your software, let people cope. But whatever motivates us to create the software in the first place probably motivates us to want people to use it safely.

And so, we do look for solutions, sometimes creative ones, but we do not because of the non-contracted nature of these dependencies. We don't have a list of who is using our software. And indeed, the software may propagate along indirect paths where some bundler, some other application maker, maybe an operating system maker is including our software inside of something else. And if we don't know who they are, we certainly don't know who their downstream customers are.

So, it's a problem. So let's look at this from the other side. If you are depending on Open-Source software, and here I'm not thinking about in my smartphone or even on my laptop, we're thinking of the traditional enterprise context where you needed something to do the work that the company is doing. And you know that there's some really good software.

RAM MOHAN

Thank you, Paul. Folks in the audience, time to grab your phone and scan this Mentimeter poll. Your responses are anonymous. No

data is held by this app. But just grab your phone. Take a look at the question while we shift to our third panelist, Mr. Singh. Yeah.

SHRI M. A. K. P. SINGH

I am Shri M. A. K. P. Singh. I am Chief Technical Officer at CyberPeace. So, since I am from power sector, I would like to correlate between the digital infrastructure and the security of the power. So, we need electricity to run routers, and we need routers to run the grid. They are both interdependent.

Power sector is the mother critical sectors. In India, we have seven critical sectors. In U.S., they have 16. If power sector fails, it cripples others. The transition from a power blackout to communication dark out is very rapid, actually.

So, like I give you an example of 2003 blackout in U.S., Canada, it was a manageable blackout, but it cascaded into collapse of much of the northeastern regional electricity system, cell towers were down, cash registers were down, ATMs were down, and public transport system was halted in Cleveland, electric pumps at the water unit is shut down.

So, that sort of impact it creates when the power is out, and we have seen many such instances. What happens exactly is the impact on the network failure is that infrastructure exhaustion. Cell towers and data centers, they have a backup facility of lead acid batteries, and they typically have two to three or four hours at the max backup.

So, if the power is not restored, then these systems do not come up, and in fact, these data centers, the servers that are there, they are very power consuming. They generate heat, and in case there is no cooling, then they execute the emergency shutdown to prevent physical melting of the systems, and killing the cloud services and internet routing.

So, that is the important impact that creates. First, moreover, the logistic collapse that is required to bring back the power itself is down, so it delays this effort to restore the grid, actually.

KATHY SCHNITT Excuse me, sorry. Can you please slow down for the interpreters?

SHRI M. A. K. P. SINGH Okay, thank you.

KATHY SCHNITT Thank you.

SHRI M. A. K. P. SINGH Like in Ukraine, when the cyber-attack was carried out, the attackers, they created a DDoS attack on the landlines, so that sort of impact can happen in a physical incident also. When this, in our 2012, there was a blackout in our country in India, we mandated that each and every installation of the power sector should have satellite phones, and because they are very handy in case when

powers are out to restore and to communicate for the restoration of the grid.

So coming to the other side of it, like when network failure happens, the power failures do happen. So, power stations rely on communication nodes for controls and communication equipment. They rely on the power grid for electricity. Failures on a limited portion of one network can cascade multiple times between these two networks in a zigzag pattern, causing widespread failures even in a highly connected mesh networks.

What happens is that we have many of the devices which are working on the internet, and though they may not be a public internet, they may be private internet, like IoT and IIoT devices. They are the eyes of the grid operator because they sense the parameters and they feed to the SCADA, on which our grid operator runs the grid.

And in case of this SCADA visibility is not there, we do follow the remote facilities, but in case of network failure, we are not able to operate remotely also our grids. So, that is the biggest cause of failure of the power in case of network failure. In case of Northeast blackout in 2003, a local physical failure in OU spiraled into a massive international crisis affecting 50 million people.

So, nowadays utilities are increasingly adopting SD-WANs to manage multiple paths. So, there has to be some resilience. If one path fails of the internet communication, others should come up so

that the powers are on. Power is on, other facilities associated will be also on.

The biggest today problem is that in the power sector grid, most of the equipment that are there, they are legacy systems because they were designed to stay for more than 35 years, but very limited cyber security bandwidth. So, there is another risk of cyber security because we are having large number of legacy systems integrated with most of the latest technology also.

So, they are the internet and interrelated and we cannot go for the blind operation of the grids. So, our digital infrastructure should be kept secure and to keep the digital infrastructure secure, we need power supply on, that's the most important.

FIONA ALEXANDER Thank you very much, Mr. Singh. I think our next speaker is Bruce.

BRUCE TONKIN Thank you, Fiona. I was asked to give a bit of a perspective from a country code operator and I work with . au for Australia. For many information-based economies, the DNS and the national naming system is treated perhaps in a similar way to having a national airline. It's become a key part of both our local economy and also our ability to do international trade. And it's starting to be treated as critical infrastructure in the same way as water, electricity, food distribution and telecommunications is treated in the country.

There is a trend beginning in some developed countries, including Australia, to begin to create legislation laws to govern domain name systems in the same way as there is laws relating to protecting water or electricity assets. And under Australian legislation at .au, we are required to take in what they refer to as an all-hazards approach to risk management.

And this is across four key areas. Cyber and information security, and we often talk a lot about that at ICANN meetings, but also personnel risks. And that could be through both a person maliciously trying to do something to the infrastructure or simply human error.

Supply chain is increasingly seen as a risk and then the risks from physical or natural hazards. When there's disasters, whether they be natural, which could be from fires, floods, earthquakes, hurricanes, COVID-like pandemics, or human based, whether they're as a result of war or as a result of cyber-attacks from criminal organizations. When these disasters occur, these actually affect multiple parts of the critical infrastructure at the same time.

So, it's not just going to affect electricity or not just affect the DNS, it actually affects both at the same time. So, there's a growing awareness that the dependencies between critical infrastructure industries have dependencies in that we may be using common cloud providers.

So, the electricity industry and the DNS industry could both be using Amazon Web Services underneath. So, if the data center goes

down, as Mr. Singh mentioned, it takes out both the DNS and the electricity network. There's also a lot of use, and I think Paul was pointing this out, but we use common software. And a case study of that recently was last year with CrowdStrike. That affected multiple parts of critical infrastructure at the same time.

So, there's an awareness that we need to look at the whole supply chain, both in terms of cyber security, but also the interdependencies, and making sure that we have a truly diverse and resilient infrastructure.

And then the other aspect of it is you can never predict exactly what will happen. So, you have to assume that disasters will happen. And it's more about practicing and restoring services when those disasters do happen. And that requires practice, not just within your organization, but you actually need to practice it with other elements of the supply chain. But back to you, Fiona.

FIONA ALEXANDER Thanks, Bruce. And our final speaker, Dan.

DAN YORK Greetings. Thank you all for bringing this panel to an ICANN event. This is a critical time for us to think about this kind of resilience.

I want to go in a different direction a little bit, and talk about in Sierra Leone right now, there's a refurbished 40-foot container mount mounted on a truck chassis. It's travelling around the country, changing the lives of women and girls. It's part of a project

called Digi truck Salon, and it provides training and information to people, many of whom are using the internet for the first time.

It brings training, it brings mentoring, it brings other aspects. And it's had great success. Fatmata, a woman who runs a business transforming shoes, learned how to advertise, and her before and after video went viral, boosting her customer base and her income.

Another woman named Mary, who's a tailor, learned how to market her designs, and now proudly models her creations in video. Her online presence has increased her sales through her WhatsApp business group. Another woman spoke about how she'd grown her revenue by 95%.

These are life-changing activities. And there's millions of other stories like this all around. And if you look at why they're successful, it's because they had internet, obviously, but they also had DNS for their courses, for their capabilities, and for the services that they continue to use in some way. This is the critical part in why we need to talk about resilience here at ICANN.

ICANN plays a critical role in ensuring the resilience and continued operation of the ecosystem around DNS and other identifiers. And yet, when we look at things, our Internet Resilience Index that we maintain at pulse. internet society. org shows that regions like Sub-Saharan Africa and parts of the Pacific region score about 30 to 40 in a range out of 100, meaning they're already operating on fragile infrastructure sometimes with little margin of failure.

When the internet goes down in any economy, it doesn't just disrupt services. It cuts off livelihoods like Fatmata and Mary. It cuts off access to government and healthcare for people who sometimes have no alternative. And as we move more and more systems to digital public infrastructure, to more and more services in different ways, we're increasing the dependence and need on having that internet access there.

We have to look at organizational resilience. We have to look at technical resilience. We have to look at human resilience, wherever it may be. There are places here we can learn. There are places all around the world as well. We also can learn a lot from emerging economies. Mr. Singh just talked about the massive outages that we've had in different places around the world.

I would point out a couple of years ago, I was documenting internet shutdowns and we watched what was a massive power outage in Puerto Rico. About 90% of the infrastructure went dark, the power grid. And I thought, well, the internet will go down, right? In fact, it dropped a bit, but it stayed going. So, I reached out to somebody from our Puerto Rico chapter there and asked why? What happened? What kept it working? His answer was that people there don't depend on the power grid. They assume it will fail. And so, they've built personal resilience with cheap solar panels and batteries to keep their Wi-Fi routers going.

The telco operators have gone and set up their own generators and systems to go and work with it. There're lessons in resilience that

we can learn from all over the space around that. And it's critical that we must. There's so much that we need to do and to think about because there's also 2.2 billion people who are still offline. And every outage that we have also erodes trust in the internet and makes the case for connectivity a little bit harder sometimes.

We're not just losing uptime. We are losing the argument that the internet's worth investing in. So, there's much we need to do and much that we can do both within the ICANN community and within the broader internet community to ensure that people like Mary and Fatmata and people everywhere have access to reliable and resilient internet. I look forward to the rest of our conversations here.

FIONA ALEXANDER Thank you, Dan. And thanks to all of our speakers. I'm going to turn it back over to Ram to do our first theme of the three that we're going to cover today.

RAM MOHAN Thank you, Fiona. We have three threshold themes for our experts today. Exploding system complexity and underfunded preventative care. Circular dependencies and supply chain risks. And finally, ICANN's role in internet resilience. To kick off our discussion, let's look at the sheer scale of the systems we operate today.

The internet is not just a collection of routers and cables anymore. It's a massive web of APIs, cloud services and third-party vendors. Paul Vixie just spoke about that in his opening statement. We need to talk about what happens when this complexity outstrips our ability to manage it. So, to the panel, first question, modern applications can depend upon 30 to 40 different APIs and third-party services. At what point does complexity itself become the threat and who is responsible for managing it? Who wants to take this question?

SHRI M. A. K. P. SINGH I will take it.

RAM MOHAN Please.

SHRI M. A. K. P. SINGH Mr. Ram, actually, when we talk about this number of different APIs and third-party services that we are available, willing to keep our systems on, we are creating a black box problem because no single person understands the entire dependency graphs, actually.

So, making troubleshooting guesswork, it is a guesswork only. And further, when we are having so many APIs we are integrating into our system for efficiency and resiliency purpose, there are potentially supply chain attack factors, actually. So, we are

expanding our trust boundaries to manage and we are not able to manage this sometimes.

And we trust on some parties like Dan York cited the example of CrowdStrike Falcon sensor, Microsoft Windows devices crashed in July 2024 when the patch that was not fully tested and pushed automatically into the kernels of the Windows and many of the flight operators, they were not able to extend the services to the passengers for issuing the boarding passes or display of their flight status.

So, that sort of environment becomes complex and we need to have less dependency on APIs and the third-party services, otherwise it will become invisible in front.

RAM MOHAN Thank you. Paul, let me ask you, do you agree or disagree with what Mr. Singh just said? And if you're speaking, we cannot hear you. We can hear you now.

PAUL VIXIE And I want to add that complexity has the role in digital systems that heat has in physical systems. It is a waste product and you can't get rid of it easily. So, the more we scale this, the more we will be ruled, our fate will be ruled by the law of large numbers so that the number of assumptions other people make about what you will do, that you never know what they are and vice versa grows without bound and has the impact that Mr. Singh was describing.

RAM MOHAN

Thank you. Bruce, do you have an opinion on this as well? Not at this point. Okay, great.

Well, let me ask the next question. Hyperscalers have the resources and operational discipline to test failure scenarios routinely and somewhat comprehensively. What happens, Danny, to the overall ecosystem when the smaller operators that they depend on don't?

DANNY MCPHERSON

Yeah, so I think that you see things like you saw with CrowdStrike, right? Where people deploy a software agent that can update inputs, modify kernels and have a staging or a test environment before they did that. And you see outages like this.

Now, that said, I'm not convinced that Hyperscalers have a much better track record than most other ecosystem operators today, given the multitude of outages we've seen of late, but they certainly have a lot of capabilities, a lot of scale and impact and consequences. And so, it's a lot more visible. So, I wouldn't call them out from that perspective, but at the same time, they tend to move quick and have big impacts when they make even small mistakes.

So, I think that it's fair with smaller folks or people with less resource capabilities don't have the same capacity. I think the onus is on everyone to make sure we develop best current practices, we design resilient and robust capabilities so that you don't have heart

failure when mistakes happen, as much as you can possibly do that. So, you're ahead of time.

RAM MOHAN

Thanks, Danny. Dan, you've been watching this and you've been measuring and looking at internet resilience for quite a while. You operate an index; you've been involved with operating an index. So from your perspective and your vantage point, what are the failure scenarios today that worry you the most?

DAN YORK

All right. You took that a different direction where I was going. I think the internet's only resilient as its weakest link. And I think in many regions, that weakest link is the small, maybe national internet service provider or IXP internet exchange point with no dedicated resilience budget in some way. I think the thing that keeps me up is the ability of organizations locally to recover and to work with us.

I think the dependencies is what we don't understand as much. And this comes back to things you said at the beginning, Ram. We have to look very holistically at how this all interconnects. What are the supply chains? What are the powers? What are the routings? What are the payment systems? How is that all linked in different ways?

I think one critical piece around this and to work with that complexity is specifically looking at how do we develop local

technical expertise? How do we create local peering infrastructure? How do we create local technical communities? How do we do capacity building to help people understand and build internet where they are?

We've seen that capacity building matters as much as equipment or protocols or anything else. We've seen repeatedly that trained local communities recover from outages far faster than those that are dependent on somebody very distant or whatever.

So, that's, I think, building on what Danny just said. There's a definite need to identify and share best practices. And there's also a need to make sure that there are people out there in the field, in there, who are able to go and build, maintain, repair, fix that internet infrastructure in some way. That makes it all more resilient.

RAM MOHAN Thank you, Dan. Carlos, do we have results from the first Mentimeter poll? That Mentimeter poll was what will be the largest cause of the next global disruption? Okay, while we wait for Carlos to bring that up, let me ask one more question to this panel.

We keep hearing that resilience is a proactive prevention problem, but also that prevention doesn't attract money. So, Bruce, who in this ecosystem on resilience, who controls budgets and what would it take to change the calculus of allocating budgets for prevention rather than allocating budgets on reactions?

BRUCE TONKIN Yeah, I think part of that is actually being able to properly articulate the risk to those that hold the budgets in a way. I mean, there is money available. And whenever I'm sort of looking at resilience things, you really need to clearly articulate the risk and explain what can go wrong and why, and how applying additional funds would significantly address that risk.

RAM MOHAN Thank you, Bruce.

SHRI M. A. K. P. SINGH May I add something?

RAM MOHAN Please.

SHRI M. A. K. P. SINGH Most of the time when, like I was a Chief Information Security Officer, most of the time when CISOs go to their Board to seek for a fund for cybersecurity measures or for ensuring their resilience, the Board always asks many questions and the finance department holds on the fund actually, proposals.

So, only when they realize when some incident happens. One of the recent incidents that happened in the JLR attack, Jaguar Land

Rover, the company suffered a loss of £1.9 billion. It is a huge loss. Even the U.K government had to come in.

At the time, that company realized that they should have spent a lot of money on that for ensuring the resilience of their manufacturing process. So before being a reactive, one has to be a proactive and really fund this budget for ensuring the resilience prevention mechanisms.

RAM MOHAN

Thank you, Mr. Singh. Carlos, I'm assuming you will put the results up when you're ready to do it. So, if we accept that complexity is outpacing our budgets for prevention, we have to look at where that complexity actually lives. And increasingly the weakest links are the invisible systems that sit entirely outside our own networks. So, Fiona, let me pass the baton to you to look at our second theme, Circular Dependencies and Supply Chain Risks.

FIONA ALEXANDER

Thank you very much, Ram. So, as you've said, this first session has sort of made clear some of these circular dependencies that we have. And we're looking at an environment where the internet needs the power grid to run, but the power grid increasingly needs the internet to recover. And it's not just physical infrastructure. It's also the Open-Source code buried five layers deep in our software.

So, first question over to Mr. Singh. The 2025 Iberian blackout shows us that power failures become internet failures which

become power failures. Does the energy sector know it has an internet problem? And does the internet community know that it has a power problem? What's your perspective on that?

SHRI M. A. K. P. SINGH

When we talk about this Iberian Peninsula mainland attack, it affected 50 to 60 million people actually. And all because of two, three things that are important to note here that most of the generation was from the renewable energy, solar and wind. They are weakly connected to the main grids and these elements are not having inertia. And that's why whenever they are out actually grid is not able to stabilize.

So, when we talk about of having a very heavy installed capacity of renewable energy, these failures will happen. And at that time, we need our digital infrastructure to be more secure. Like in this case, this autonomous system stopped announcing IP prefixes as soon as the power failure happened actually. So, in case like the Portugal and the Spain, the Portugal internet traffic dropped by 90% and the Spain drought was less severe all because they had more backup power supply backup.

So in the case of power outages also, if you have a better backup supply, then you will be able to maintain your digital infrastructure. And when the digital infrastructures are up and on running, you will be able to restore your power supply in a quicker manner. That is the first and foremost learning from it. And we have already seen that many of the devices that are there, they require a minimum

amount of power also. Like when we are doing switching, the battery level should be 75% to switch on and switch off our circuit breakers in the power sectors, which are important to bring and restore the supply. So, that's what infrastructure is requirement is.

FIONA ALEXANDER

Thank you very much for that. ccTLD operators sit at a critical juncture between ICANN policy and national infrastructure. How exposed are registered operators to supply chain risks that they can't even see? And this question is for Bruce as a CC operator.

BRUCE TONKIN

Yeah, thank you, Fiona. I think one of the key things there is that you need to actually ask your suppliers to draw you a map of how their service is made up. In other words, a network design or a physical design and the key vendors that your service provider uses to provide the service.

One of the issues, we talked a little bit about complexity earlier, but what I've observed is that in any particular organization, there's one or two people that in their head understand all that complexity. If you lose one of those people, or they're not available because they're out of contact for some reason, you're in trouble because a lot of it's not written down. And so, there's no backup if that key person is not there.

So the key both for your own infrastructure, but especially your supply chain is to get them to provide you with the information on

a diagram, if you like, of their system and their suppliers, get them to articulate to you their risk management plan, get them to provide you with copies of audits that that might have done through external services, such as an ISO 27001 audit, and get them to work with you on cybersecurity exercises so that you actually understand what is in their supply chain.

FIONA ALEXANDER

Thanks very much, Bruce. So, a key takeaway here is that, we're vulnerable, our networks are vulnerable to cascading failures from outside of our sectors, even if we have everything perfectly configured in our own networks. But we're here at an ICANN meeting today. So, we have to ask ourselves, what's the specific job of ICANN and the ICANN community in all of this, which goes to our next theme. Thank you.

RAM MOHAN

And before we do that, Carlos, shall we go to the third Mentimeter poll? Are you ready for that? So, we have another poll. So, audience, please pick up your phone and scan this code. And the question that we're asking when it does show up on the screen is, if your region's primary power grid or cloud vendor went entirely dark for 72 hours, how confident are you that your core services would survive?

So that's a question, it'll come up on the screen. So, while we do that, this is our final discussion topic today. Let's bring it back to

ICANN. We cannot fix the world's power grids. We cannot patch every Open-Source library. We cannot solve every geopolitical problem that happens. But we collectively are still stewards of the internet's Unique Identifier System.

So, where does the ICANN community's mandate intersect with the reality of environmental fragility that is seen so clearly in the world around us? So, Danny, what would it actually take for brittleness in systems like RPKI or DNSSEC to cascade into something significantly disruptive?

DANNY MCPHERSON Did I unmute? Yeah, there we go. So, I think the DNS protocol itself is inherently robust. And both implementation and operational practices make it even more robust. There's a caching layer to absorb failures and entities that operate core elements of that infrastructure have proven operational prowess.

I think if you look at the uptime and track records of the root server system or some registry operations there, they far exceed any cloud operations or other things. So, I think there's a good track record there. That said, there have certainly been DNSSEC related failures, but most come down to experience and basic operational hygiene.

There are certainly scenarios you could conjure up where RPKI failures trigger routing instability, which causes DNS and everything that relies on routing to work, to break, which inhibits RPKI from being repaired because it relies on the DNS to work,

right? So, I think that's kind of a worst-case scenario. But that said, I think the very reason today that most operators have implemented buffers or other controls such as downgrading routing preferences rather than hard fail scenarios are, which in and of itself represents a downgrade attack in the securities that those controls provide you.

But those things provide some robustness and factor prudent operational trade-offs. But I think that as we see RPKI relies on DNS and DNS relies on routing and circular dependencies are problematic when you're trying to engineer both recovery plans or resistance to failures, but certainly resilience in the face of failures so that you can downgrade and recover from those and provide some level of service and be able to return to normal operating posture. So, I think that's a fair question, Ram.

RAM MOHAN Thank you, Danny. So, Dan, civil society and users in emerging economies are often the most exposed when systems fail. And also Mr. Singh, this is also something that I'm going to come to you in a moment, but let me go to Dan first. What are the human costs that we are not talking about enough?

DAN YORK So, great question, Ram. And I think the challenge is that we're not, I mean, the human costs are that we're not changing the world. We're not making the effect of things. If you look at civil society, if

you look at the organizations in the nonprofit sector first, the challenge is they just don't often have the resources of enterprises.

Their funding, their efforts are focused on their mission, the program, not necessarily on IT or on the IT infrastructure, whether it's feeding the hungry or teaching digital skills, advocating for human rights online, whether it's a school, a church, a library, whatever, the focus is on the mission, changing the world takes priority.

IT infrastructure is usually a lower priority. Often in looking at the question that you just asked in the Mentimeter, often those are reliant on third-party systems. They can't necessarily bring themselves back up in some way.

So this is where local technical communities, local groups like that are so critical in being able to help with that recovery and building that human resilience to be able to go and help work with that. I think that, you ask in this section about what can ICANN do, I think the ICANN organization and community can play a vital role here.

Ensuring a resilient DNS and identifier ecosystem is critical and there is, we have this large and global community for ICANN that can help. Danny mentioned earlier about best practices. I think there's a tangible action that ICANN could take. One is, of course, looking at these dependencies and the pieces, but what if the ICANN community could identify the potential points of failure in the different parts of the identifier ecosystem?

Identifying best practices for each segment, whether it's root servers, registries, registrars, ISPs, recursive resolver operators, businesses, nonprofits. Then what if we could develop those within the ICANN community and then promote those best practices out through the various different constituencies and stakeholder groups?

The ISP constituents could talk to the ISPs, the BC to businesses, the non-commercial stakeholder group could reach out to nonprofits, on and on. You could be able to go and take those best practices and look at how does each part of the ICANN community build resilience to ensure the continued operations and resilience of DNS.

I think that's a very tangible thing that ICANN could go and do within that because those human costs are the cost of not delivering on those missions, not delivering on what the civil society is looking for. And as we talked about earlier as well, with emerging economies, very often they are more dependent on some of those larger scale systems. We need to build that local expertise, build that local human capacity, and that's how we make things more resilient.

RAM MOHAN Thank you, Dan. Mr. Singh, do you want to speak just briefly about this question about the human cost of resilience?

SHRI M. A. K. P. SINGH

See, I will give you a classic example, like when the power supply gets affected. Like I take in the morning, in the welcome session, it was mentioned that half of the data centers of India are in Mumbai. And you know, in 2020, there was a six-hour outage in Mumbai. And you know that how much loss of the data may have happened if this power outage may have continued for a longer time, actually.

And especially in the war conflict zones, like recently that's going on in various parts of the world, where due to disruptions, most of the digital infrastructure facilities are not available. Like Fiona asked me about Iberian, actually, when this outage happened, people were not able to buy even their bread and butter, actually, because everything was digitalized.

So, no internet, no one can do the transactions. So, these are the costs. And moreover, the humanitarian aid that we want to supply, also we cannot supply under these circumstances. And in fact, there are other angles to these issues, like this, when our systems are running in a degraded mode during this power outage or anything, so cyber-attack, are more active, hackers are more active, like whenever we, recently we wanted to extend the humanitarian aid to Myanmar, our planes carrying the humanitarian aids, they were affected by this GPS spoofing, actually.

We could very land after manual mode operation. So, these facilities get affected, and many a times they may turn into disasters if we don't have some backup facilities.

RAM MOHAN

Thank you so much. We have the fourth Mentimeter poll up. It's up on the screen. And what we're asking there is, looking at the broader landscape of internet resilience, where is the ICANN community's most critical blind spot now? So, that's a question.

So now let's turn to the community. There are two mics here in the center aisle. So, please, if you have any questions, come up here to the microphone to ask it of us. And for remote participants, please use the Q&A pod. We have only a little bit of time, so please make your questions succinct and brief no more than 90 seconds. Are there any questions from the audience? Kathy?

KATHY SCHNITT

Yes, Michael Palage, you may unmute and ask your question.

MICHAEL PLAGE

Michael Plage. Can you hear me?

RAM MOHAN

Yes.

MICHAEL PALAGE

Excellent. Thank you, Ram. In today's opening session, we heard from APNIC about the critical roles of RIRs in the internet ecosystem. My question is, why was that second N in ICANN largely overlooked in today's discussion? Second follow-up question,

unlike the names where ICANN has legal agreements with most of the gTLDs, ICANN only has an MOU with the NRO, which is a non-legal entity.

So, from a supply chain standpoint, does that represent a particular point of vulnerability? And then the third question, what is the potential antitrust considerations for ICANN and the operators of Internet Unique Identifiers? Is that a security or stability threat? Any speakers willing to speak to any of those three questions would be appreciated. Thank you.

RAM MOHAN Thank you, Mike. Danny, let me pivot to you and ask if you want to cover one of those three questions.

DANNY MCPHERSON Yeah, no, I'm happy to. I mean, we spend a lot of time working with members, from an operational perspective in my day job, a lot of time working with three of the RIRs for which we're members and follow a lot of their developments very closely. RPKI, which has more operational impacts on the infrastructure, more direct operational impacts on the infrastructure we operate has concerned us.

And we want to make sure that that infrastructure is robust and secure. And the investments in that are important. And the people that operate that hold themselves to a standard and illustrate the security and operational prowess that we would expect from any of

our service suppliers. And so, we do spend a lot of time on that. And I think it's more and more relevant now than it's ever been, right? I mean, five years ago, I didn't have to worry about RPKI at all.

And now I have to worry about my operational attack surface and the capabilities those RIRs provide and plan around failures of that. I do think the RIRs have done a number of things to force robustness of the infrastructure.

One of my opening comments was loosely coupled systems and about some of the buffers that are in place for some of these controls in case failures occur. And Aaron, for example, forces that with some planned outages of their infrastructure. Not luxury registry operators have, unfortunately, or fortunately, I guess, but I think the RIRs are definitely improving their capabilities there.

I think both the state of the supply chain for software that enables the RPKI and the investment and the funding of the RIRs themselves is really important to make sure that that operational infrastructure that they provide is continues to enhance its capabilities and remain secure and robust. So, I think that's all I'll say about that.

RAM MOHAN Thank you, Danny. Let's take a question from here in the room.

ANAND RAJE Hello. Anand Raje from India Internet Foundation for our records. So, we are surrounded with APIs and we are talking about that.

RAM MOHAN Slow. No, speak into the mic.

ANAND RAJE Hello?

RAM MOHAN Yes.

ANAND RAJE Yeah. And system services over internet identities all mostly depend on centralized trust architectures. My question to the panel is, what is the impact of centralized trust architecture on regional internet resilience?

RAM MOHAN Thank you. Paul, do you want to take that?

PAUL VIXIE I will, but can you repeat the question? Repeat the question.

RAM MOHAN What is the impact on the centralized trust architecture has on regional internet resilience?

PAUL VIXIE

By default, it's pretty concerning. In other words, we have seen times when there was not adequate resilience of connectivity between some region and the rest of the world. And there was a couple dependency such that local systems could not find other local systems or could not decide whether to trust other local systems because neither one of them could reach a very distant system.

Again, this happens by default. It is something that every designer must look for. And that is why designs, not just implementations, deserve to be red-teamed. In other words, they deserve hostile testing by people who are trying to find these flaws before they operate.

RAM MOHAN

Thank you, Paul. Kathy, any other questions from online?

KATHY SCHNITT

We do have an online question for Bruce. Australia has elevated cybersecurity to a cabinet-level portfolio with a dedicated minister. Has that change meaningfully strengthened the government's approach to DNS security and broader cyber resilience, or is the real challenge still an implementation across agencies and industry?

BRUCE TONKIN

That is a tough question. I think what Australia has done from a government's point of view is it's created a Department of Home Affairs and they've tried to aggregate a lot of the security functions across different agencies into that department. And through that department, they created a piece of legislation called the Security of Critical Infrastructure Act.

And so, that's the main thing that impacts us as a registry operator, which is, if you like, a community of critical infrastructure operators. The Minister of Cybersecurity, though, remit is broader than that, which is across the whole of industry, not all of which would be considered critical infrastructure providers. And that particularly relates to small businesses. And so, there's also a parallel effort in how do you raise the awareness of cybersecurity amongst small business? And what practical things can you do to help small businesses improve the security of their system?

So, I would say that Minister's probably more focused on that broader small business cybersecurity, whereas our interaction as a registry operator is with other critical infrastructure providers through the Department of Home Affairs.

RAM MOHAN

Thank you, Bruce. Let's take a question from the audience here.

IDIL KULA

Hello. This is Idil Kula from Turkey for the record. I'm an ICANN Fellow. So, all of the panel, you're talking about the resiliency,

robustness, and Continuous Operational Internet Infrastructure as a whole. And as you again said, it's the whole network of not only infrastructure, also APIs and cloud services and third-party vendors.

So, the only thing that I didn't hear is, you're on supply chain risks and energy risks. But in order to internet to go on and have resiliency, we actually need environmental and ecological resiliency first, because we depend on environments to get the energy to have resilience and continuous internet.

So, how do you think that ICANN can encourage all the stakeholders in order to have more sustainably responsible practices? Because we are all a community from all over the world. If there's one party who can enforce and encourage people to have more sustainably responsible practices, it is the place that I feel. It should be the place.

So my question, how can we do the encouragement altogether? Because if we wait for the governments or regional actors to enforce the climate responsibilities, we will obviously be too late. And at the end of the day, if we don't have ample water to get the supply chains go on, we don't currently have any continuity of internet.

RAM MOHAN Thank you. So, let me refer this question to you, Dan. What do you think ICANN can do to help with environmental ecological resiliency?

DAN YORK How much time do we have, Ram? I think there's a larger question that, we couldn't hear the actual question online, Ram. So, if you could repeat a bit of it.

RAM MOHAN Yes, I summarized it for you. What do you think ICANN can do to help with environmental, climate change and environmental and ecological resilience? So let me just -- because we're just running out of time. So, I'm just summarizing it.

DAN YORK Okay, I appreciate that. So, I think there's a great amount of work happening within the larger internet ecosystem around these kinds of climate issues. Some of them are looking at green computing, how to operate data centers, how to operate systems at a better level that's more carbon friendly, that's using less energy.

There's a whole strain of things there. I don't have specific recommendations right now, except to say that as you look at the whole supply chain, as we look at all of the different pieces and systems, each one of those has a place in which they can look at what are their impacts to the climate crisis? How much energy are

they using? How could they lower their energy footprint? How could they make systems work in a more carbon friendly way?

All of those different kinds of things can be done at every level of the hierarchy, whether it's registries to registrars to individual ISPs to people using CDNs or operating their own authoritative servers. There're places in there where all of that can be considered. That could be another thread of work that ICANN could take on to look at how could these systems within the DNS and identifier ecosystem be made more climate friendly.

RAM MOHAN Thank you, Dan. Carlos, let me come to you and ask if you could show and share with our audience the results from the Mentimeter polls. So, here is what you said about what you believe will be the largest cause of the next global disruption. Okay, let's go to the next response, next question.

SHRI M. A. K. P. SINGH Hello, sir. My name is--

RAM MOHAN So, hold on. I'm just going through the Mentimeter question responses. And is there any other poll response? Please go to the next one. So, by a pretty significant amount, what's being said is that cross-sector coordination, communicating with energy, telecom, other sectors, cross-sector coordination is ICANN

community's most critical blind spot. That's what this poll is showing.

And is that it, Carlos? Okay, great. So, thank you very much. Let me shift to our panelists now. And let me start with you, Bruce, first. And this is a question I'm going to ask all the panelists. If you had just a little bit of time to speak directly to ICANN leadership after this plenary session, what would you tell them needs to happen first?

BRUCE TONKIN I think we need to put effort to map out the supply chain of the registries and DNS providers and look for key dependencies, then run some scenarios if some of those key dependencies had issues. So, I'll give one example is a lot of us use BIND as a piece of software. What would happen if there was a problem with BIND and run some scenarios?

RAM MOHAN Thank you. Paul, what would you tell ICANN leadership needs to happen first after this session?

PAUL VIXIE We didn't talk very much in this session about the regulatory pressures, but I know that something like COICA can come out of nowhere, protect IP. If we don't go to California and say, all right, you've just asked for age verification, including on Open-Source, including non-contracted systems, that can't work. What else are

you interested in so that we can hear about it before you decide to pass it into law?

I think we need more broader outreach to the worlds, especially the democracies to find out what it is that they wish they could get from the internet so that we can start the process of either building it for them or telling them why it's not realistic.

RAM MOHAN Mr. Singh, what would you ask?

SHRI M. A. K. P. SINGH Just as the Mentimeter results showed, actually, I would like to say that failures in power system may cascade across the dependent critical infrastructure. So, that may impact the nation also. We need to understand how entities like electric facilities, communication hubs, and many service providers come together to support critical functions to keep the digital infrastructure on and up running.

RAM MOHAN Thank you. Dan, what would you ask?

DAN YORK I would say three things. ICANN needs to look at how to build its organizational thinking around resilience and putting that into more of a strategic thinking or element. It needs to look at technical resilience. What Bruce just said and Mr. Singh about

mapping the hidden dependencies of DNS and the identifier system, and looking at those best practices I mentioned earlier and the human resilience.

So, it's that organizational, technical, human resilience aspects, looking at how do we go and do that and making use of the global community that we have. And I think there's a lot of organizations out there that are working in this space that ICANN can be partnering with in some way. But if it does that, then we'll get to a spot where we can ensure that people everywhere have access to reliable and resilient internet.

RAM MOHAN Thank you. Danny?

DANNY MCPHERSON I think various elements of what we've talked about are already embodied in ICANN's strategic plan here, I think. I think it's clear that ICANN and this community from the technical systems and the technical remit have done an exemplary job of operating the infrastructure in a secure, stable manner for, you know, for as long as we have. I do think that there's some broader opportunity for focus on externalities of things that impact the system. I'm not sure. I see, you know, in the survey here, the 38% cross-sector of coordination.

I think one of the things that's lost in some of that is that a lot of the responsible entities that are stakeholders in this ICANN community

spend an inordinate amount of time focusing on disaster recovery, emergency communications, business resilience, working with partners, you know, the what-if scenarios and operating resilient systems.

So, I don't know that ICANN needs to do that directly, but certainly fostering that and the supply chain elements of that and so forth. But I think that more strategically, the thing that I'm not sure I see is the trends and threats forecasting, a strategic outlook of, you know, these trends. What are the geopolitical shifts and emerging technologies, the economic disruptions that could destabilize ICANN in this community?

I think understanding those external forces and then figuring out what's within the core remit of ICANN and the ICANN community is something that's actionable within the ICANN community here.

RAM MOHAN

Thank you, Danny. Let me ask all of you here in the audience, here in the room, raise your hands, after the last hour, do you feel that ICANN needs to make internet resilience a strategic priority? Okay. Okay, lovely. Fiona, I'm going to switch back to you for any final comments.

FIONA ALEXANDER

Oh, I think I'm going to forego those given that we're a little bit over time, but thank everyone for their great presentations and hopefully for those online in the room, online and in the room, the

	session was helpful to sort of stress the importance of everyone having a role in internet resiliency.
RAM MOHAN	Thank you very much. Thanks for all the panelists and we are adjourned.
KATHY SCHNITT	You may stop the recording.

[END OF TRANSCRIPTION]