ICANN84 | AGM – ccNSO: IANA Disaster Recovery
Wednesday, October 29, 2025 – 13:15 to 14:30 IST

CLAUDIA RUIZ

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

Please observe the following guidelines to participate in this session. They will be posted in the chat for your reference. During this session, questions or comments submitted in chat will be read aloud if put in the proper form as noted in the chat. Interpretation for this session will include English, Spanish, and French. If you would like to speak during this session, please raise your hand in Zoom.

When called upon, virtual participants will be given permission to unmute in Zoom. On-site participants will use a physical microphone to speak. Please state your name for the record and the language you will speak if speaking a language other than English. Thank you and with that I will now hand the floor over to Peter Koch. Thank you.

PETER KOCH

Thank you, Claudia. Good afternoon, everybody. Welcome back from your lunches. My name is Peter Koch. I work for DENIC, which is Germany's TLD registry, and I'd like to welcome you to this session. The session will be about Disaster Recovery and in particular the potential role of IANA. I will learn about ccTLD experiences and get information from IANA and from ICANN.

I would like to put this a bit into context because some of you may remember that we had a policy Gap analysis Working Group that concluded by producing a set of recommendations, and these recommendations led to the definition or chartering of currently two study groups, one of which is the study group on IANA's role in Disaster Recovery.

Now this session was being worked on before that scheduling had taken place, so we are approaching this topic more or less from two sides, but the, not but, but and the study group, members of which I see a couple in the room, will take results or experiences shared and voices raised here as part of the input to the work of the study group, and I can say a few words about the study group at the end maybe.

So, just a quick look at the agenda. Régis will give us a TLD Ops perspective. You know that TLD Ops is a standing committee of the ccNSO. Kim Davis will shed some light on IANA perspectives. We get information from Francisco Arias about what is happening or what is offered to, well not offered to actually, but what is current

practice in the gTLD space as an information point for further discussion.

Then again, Régis will, this time with a different hat, share observations in his role at AFNIC, and in the end we'll wrap up and summarize, and that will then be my task together with hopefully all of you who listen, contribute, and share experiences. Thanks. So, Régis, are we good to go? Then this is yours. Thank you.

RÉGIS MASSÉ Thank you, Peter. Hello, everyone.

PETER KOCH Hello, sir.

RÉGIS MASSÉ Okay, it's a cyber-attack in the room. Okay, hello, everyone. I'm Régis Massé. I'm the CTO of AFNIC, the .fr registry, and for this first part of my presentation, I will take the cap off the TLD Ops chair that I have since nearly two years now.

For newcomers, maybe in the room, just to be very quick on that, the TLD Ops group is the operational security community for ccTLDs. So, the objective, the main objective is to provide a contact list of contact and mailing lists to share information, and trust platform to cooperate and information sharing among ccTLD operators to manage security incidents, enhance DNS reunions, coordinate response to threats.

And the participation is just restricted to ccTLDs, not only the ccNSO, but all the ccTLDs, and I will be back on that. It's important.

So, the main objectives are, as I said, is to make a trusted list of contact to share and to fight against attacks with operational people from the ccTLDs. So, we give this list of contact, and after that, we have started to develop delivery and tools for the ccTLDs. We have made a DDoS attack delivery, something to help ccTLDs to fight against DDoS, and we have worked on the RBCP, especially for five years now. Next slide, please.

So, just to be sure to have a, to share a comprehension of business continuity and Disaster Recovery. Business continuity, this definition is not perfect, but we can say that is the capability of organization to continue delivery of products or services that are important for the ccTLD registry operators, business and stakeholders at acceptable predefined level following an instructive incident.

Okay, so I say we must continue to work with, we must continue to deliver the DNS services, we must continue to deliver the record, the recording of the names, and we work, we must work with the stakeholders. And in this business continuity, we've got Disaster Recovery plans that are related but not interchangeable.

Business continuity is a plan of action, but Disaster Recovery has procedures and plans, and business continuity contains some plans, but you've got technical plans, you've got human resource plans, you've got communications plans, and business continuity

englobes all these kinds of plans. It's a way to make a difference, because sometimes the two notions are taken, and we can confuse on this kind of notions.

So, we made some deliverables at the TLD Ops group, with the TLD Ops groups. We made a playbook, and all these kinds of things are available on the link on the on the Confluence web page we've got, hosted by the ccNSO and ICANN, of course. We've got a playbook. A playbook is to define templates and define what we have to be, to be prepared for a disaster, and having a list of contacts, for example, making some procedures to be prepared to find and to restore the system if it's broken.

And after that, we have made tabletop exercise documents. The idea is to train and to simulate exercise with action cards. It's a tabletop exercise. It's, there is the scenario, of course. We have five step scenarios. So, when we played this tabletop exercise, every 20 minutes, we've got new information. So, the players can decide what to do.

And about the tabletop exercise, the idea is also to simulate a registry compromise. So, in the web page, you've got two scenarios for the moment, because we played two sessions during ICANN. During ICANN66 in Montreal, and during ICANN81 in Seattle. Back again. And the second one is important, because it was the, in the cooperation with the European TLD-ISAC.

So, that's why there are the two logos on the cards. If you see the cards on the right, it's the four role players can have when they play

during the TTx. Technical, of course, but also management, communication, and legal or regulatory. And it's important to cross these profiles in each team of the game, because we can, with that, having a real experience and be sure that all the parts of the crisis are addressed during each step of the game.

So, just have a look at the last TTx. Some of you will recognize them on the photos, of course, but the idea is to play the game. But the second part is also very important. At the end of the game, it's to analyze and make a re-text on why those groups take those choices. And you see that if we have, at the last exercise, I think eight teams were played, and we have eight different answers. And it's very interesting to see.

First of all, during the game at ICANN, I like that because we share registries, and it's a good way to share information with other ccTLDs in the ccNSO. And the second thing is to say, okay, we are big registries, we are small registries, but yes, okay, we have the same problem, and yet we will address the problem differently. And I think it's very interesting to learn and to exercise and to practice about these kinds of things. Next slide, please. I think it's okay for me.

PETER KOCH I think you're done, right?

RÉGIS MASSÉ Yes.

PETER KOCH

Thank you very much, Régis, for that first contribution and the experience and an example of active exchange from the TLD Ops Committee. I would like to allow clarifying questions if we have them at the moment, but I would defer discussion to the end of the session.

Are there any clarifying questions? I don't see any in the room. And I don't see any in remote. So, with that, and the slide is already there, I would like to invite Kim to share AINA's perspective. Kim, the floor is yours. Thank you.

CLAUDIA RUIZ

Thank you. A quick note from our interpreters before we continue to please speak slowly. Thank you.

KIM DAVIES

Thanks, Peter. So, I'm going to talk about Disaster Recovery from an IANA perspective. I imagine you're all familiar, but predominantly this is from the perspective of administering the DNS root zone. So, the genesis of discussions that I've been involved with, with the ccNSO in recent years, dates back three or four years ago when there was a particular operational incident with one ccTLD where IANA needed to take action to restore service of a ccTLD in a relatively unique situation, but a situation that the policy really didn't cover.

And in tackling this operational reality, we reached out to ccNSO leadership and explained what we plan to do. Thankfully, that issue was resolved and isn't the topic of today's discussion. But as an outcome of that collaboration with the ccNSO leadership, IANA was invited to contribute some of our more general experiences in day-to-day operations where we perceived there was some policy Gap that meant that we weren't necessarily either empowered or didn't have a way to address operational challenges that we ran into.

So, a policy gaps analysis Working Group was established and really sort of kicked off with IANA presenting a number of observations of areas where potentially there is a lack of policy, which is not to say that IANA can't do anything without that policy, but the ccNSO may choose to look at the situations and find that policy would actually be desirable.

So as part of that exercise, we identified a number of opportunity areas. And one of those was, I guess I would call it a lack of recovery options available when a ccTLD isn't operating correctly. Now, when we think Disaster Recovery, I think we immediately think to a natural disaster, some kind of earthquake, flood, those kinds of things.

And obviously that is certainly a disaster that we would all want to recover from if it was impacting our ccTLD. But when I think of disaster, I think of a slightly more expansive definition of which that is a part, but the kinds of disasters we've seen over the years that

either merited an IANA response, or at least the parties came to IANA seeking a response, include other kinds of scenarios.

One such scenario is a fundamental business failure of the ccTLD manager. The company or the entity is no longer operating. Such scenarios doesn't mean that the TLD is not resolving. Often situations are complex. Maybe there's a registry service provider that's still operative. Maybe there's name servers that are still operative. But nonetheless, the ccTLD manager itself is no longer operating.

Another situation is some kind of unfixed serious violation of the common set of global policy requirements that every ccTLD has. And I'll get into the details in a forthcoming slide about what that might involve. So, in this context, with this more expansive view of what Disaster Recovery might entail, this was the question that I had posed to that Policy Gaps Working Group.

What, if any, requirements should be established around Disaster Recovery and or the ability to sustain ongoing operations of the domain in the case of disaster or non-compliance with global policies? So, from where I come from, that's sort of the framing question that ties this subject together.

PETER KOCH Can you go a bit closer to the microphone? It's a little bit difficult to hear.

KIM DAVIES

I can. Thank you. So, when we talk about reasons we might need to step in, in the case of a ccTLD operation not operating as expected, there is a strong connection to the revocation policy. Because the revocation policy at its heart is a set of last resort actions that might be taken if a ccTLD isn't operating in an appropriate way according to global policy. And ccNSO created some work that was published in 2013 that provided the grounds for which revocation might be the ultimate outcome.

And essentially it is when IANA deems that either the conduct of the ccTLD manager imposes serious harm or has a substantial adverse impact on the internet community by posing a threat to the stability and security of the DNS, or where the ccTLD manager is failing to perform objective requirements such as having appropriate internet connectivity, having properly configured and administered zone files and name servers that are capable of performing expected name resolution tasks, having operative points of contact and meeting minimum local presence requirements such that the manager is accountable in the relevant jurisdiction.

Such failures must be either egregious or persistent. So, that is the basic framework in which we look at cases that might be subject to revocation. Now this revised guidance has now been on the books for 12 years. Has it ever happened that we've revoked a ccTLD? No. But cases have certainly been explored and applications have been made to IANA to consider ccTLDs for revocation action.

You might be asking why am I raising this in particular? I think the reason I want to raise it is that even in situations where the grounds for revocation might be incontrovertible in that there's not really any dispute that a particular ccTLD manager is subject to a revocation action, the practical reality is that even if IANA were to make that determination, it is hard to envisage a situation where IANA could actually revoke a ccTLD because there is a lack of options available to perform a revocation while still keeping a ccTLD operating.

Some of the scenarios where this can be a challenge we could identify, and again this is hypothetical, I'm not suggesting this has actually happened, but it's certainly scenarios we've explored. There could be an issue that we've identified to a ccTLD manager where we've identified there is a clear breach of the criteria at the top of the slide. As per the policy, we need to give the ccTLD manager a reasonable opportunity to cure the issue, give them a reasonable amount of time to fix the issue, but the ccTLD manager may not simply cure it. They might not respond to us or they might say well I don't care, I'm not going to fix the problem for example, I'm just not going to do anything about it.

In these scenarios if they're not cooperative with IANA they're very unlikely to be cooperative with local parties that are seeking to remedy the same situation. I note that ccTLD policies generally favor local action over coming to IANA and certainly that's what we

promote as well, but usually they come to IANA after they've exhausted local remedies for a particular problem.

And then specifically I wanted to draw attention to the case of jurisdiction. We do see rarely cases where the ccTLD is simply operated outside the jurisdiction of the country and so in those situations' local relief, you know you can imagine for example a court order, could be issued but it's completely ineffective if the ccTLD manager is outside the jurisdiction of the country.

To be clear this expansive definition of disaster does include things like natural disasters where ccTLD infrastructure might be severely compromised, flood, earthquake, utility failures, things like that. War is something we're exposed to from time to time, could be personnel relocated due to just to ensure their personal safety. Often the environment is very dynamic, changing relatively rapidly.

Often in these kinds of situations what ties them together is it exposes a single point of failure where ccTLD manager, whether by accident or that's just the operational reality, is reliant in a in some way on a singular location. That location is no longer available and that obviously presents a significant problem.

We talked a little bit about business failures that the company or entity has ceased operations. You can also envisage a scenario for example where the entity might be operational but fundamentally prevented from doing their job but they might be under some kind of court order to prevent them from taking some kind of action.

I think another related issue and these were the other questions we presented to the policy Gaps Working Group is that you know many ccTLDs want to do the right thing here and you heard about the work that happens in TLD Ops and in most cases, every ccTLD managers want to do what's right, they want to preserve operations and in that context.

We've been approached by a number of ccTLD operators who have thought this through a lot and they actually have very defined plans that in these kinds of business failures or scenarios like we've identified other parties in the country that we work with, and maybe we have a relationship with, that if we're incapacitated in some way, we have a relationship with them and we want them to step in, in the case of an emergency.

And they are essentially coming to us saying, can we set up a private relationship where you IANA will go talk to this other body, and work with them in the case that we're not able to do our job. But there's no policy provision that would permit IANA to essentially skip. In the case of a ccTLD transfer, there's a big policy there that says, you need to do this deliberate due process it takes, in the order of months needs to go through all this review, board review, etcetera.

There's no real policy on the books that says, in an emergency with the either express consent or the previously given consent of the current manager, IANA would be empowered to take certain actions to restore service on an expedited basis. So, the questions

that we pose there is, should there be any policies regarding how these kinds of arrangements are made, and is IANA empowered to establish such arrangements.

Should such arrangements providing for temporarily circumventing policy requirements, should there be such arrangements in necessary emergencies. A follow-up question is, if we were allowed to do such arrangements, should they be private, should they be transparently reported as part of our public reporting, are there some kind of accountability requirements around them.

So, I mentioned before that, we always favor local solutions that IANA really should be a last resort to these kinds of situations but are they the complete answer. The general policy is clear. ccTLDs are designed to be administered and overseen locally but the practical reality is, not every country has the same level of sophistication to do that effectively, and the practical reality is that, if the ccTLD is in some kind of compromised state, maybe the local internet community hasn't done the necessary preparation, maybe the ccTLD manager doesn't have comprehensive Disaster Recovery plans, who do they come to?

They come to us and they're looking to us for solutions and today often, we just have to say, sorry, there's really nothing we can do and I think when we're talking about ccTLDs, I think for every country you are critical infrastructure.

I think we would all agree that we want ccTLDs to be operative and we need the tools in place that in these scenarios which are rare but that we want to be able to restore operations in some way. And I think part of the discussion that this session is kicking off that will happen in the months to come is, what is what is the role of IANA, what are the roles of ccTLDs, what are the things that are addressed locally but when local solutions fail, what are the kinds of situations that need to be addressed at the global level.

Maybe that is my last slide. No, this is my last slide. So, what do we do today. So, we have these discussions privately with ccTLD managers or prospective ccTLD managers and when asked, we informally advise that parties in the country, ccTLD managers consider local mechanisms. For example, establishing local escrow. We've noted and part of the challenge we face is that even if parties are cooperative today, there's no guarantee that for example 10 years from now, that will be cooperative.

So, in a sense when devising these kinds of scenarios, you have to assume that relationships might break down, that you need to have options available to retain service when those relationships are no longer viable. And one thing we see more than others is that, you as a ccTLD manager for example, might be highly reliant on a registry service provider and that registry service provider might not be in your jurisdiction and you might have a contract with them but if they're not a local company, they're not in your country, again, if that relationship sours, maybe they'll just say well too bad.

This might be a not be a classical definition of a disaster to recover from but I can assure you in such scenarios, the ccTLD manager considers that disaster when their registry service provider has gone rogue. So, this is a situation that I think sort of falls into the general area of problems to be solved here, but to be clear, IANA is not looking to or has no mechanisms to be a recipient of escrow.

We're not seeking to take control of any ccTLDs directly ourselves. Some have asked us to. Some have said, well, we want IANA to step in and run our ccTLD if we fail and that's not really in our competencies I think we're looking for local alternatives where they're available so just to reiterate a point I made earlier , if there are no local mechanisms to move the ccTLD within the country, then we can decide that a revocation is absolutely warranted but it's effectively unobtainable, because IANA can't compel activity by people inside the country.

We can't force a registry service provider to hand over business records for example. This this is beyond our capacity. So, it really relies on mechanisms being in place in advance that can then be triggered in these kinds of scenarios when they happen.

So, with that said, everything I just mentioned was about ccTLDs. We do deal with the failure of gTLDs as well in our role as root zone manager, and there is a structure in place with mandatory escrow. There're clearly defined ways when IANA can step in on very short notice to bring back operation of a gTLD. And to explain all of that and more, the next presentation is going to be from my colleague

Francisco, who can explain what happens in the gTLD space within ICANN. So, that's the end of my presentation. Thank you.

PETER KOCH: Thank you, Kim, for providing a lot of perspective, I would say. I see already two hands in the Zoom room. If you're in the room and want to raise your hand, you need to wave. Otherwise, I'd probably not be able to recognize. And we have one question already in the Q&A pod, which I'll give the floor to first with the asking the secretary to read that question. I'll try, we're good on time, I'll still try to keep this to immediate reactions. We have one more time slot towards the end for broader discussion. But Joke or Claudia, could you read the question from the Q&A?

CLAUDIA RUIZ: The question is from Dr. Gopal from New Delhi. Is there a time limit specified for disaster detection and recovery?

KIM DAVIES: From an IANA perspective, no. I mean, in a very finite sense, if you need to make a root zone change on an emergency basis, there are SLAs on IANA to do that quickly. But I think the kinds of scenarios we're talking about is not really related to our ability to rapidly change the root zone, which we certainly can do. It's around all the other pieces, which there's no really defined timeframes that I'm aware of.

PETER KOCH

Thank you, Kim. From the perspective of the study group, I would say that is perfect input to the work of the study group, because thinking about what exactly or broadly a disaster is, is part of the mandate to think about. Then I have Chris Disspain, please.

CHRIS DISSPAIN

Thanks, Peter. This is Chris. Kim, thank you. That was a really interesting presentation. I just have, I suppose, really a couple of points. I acknowledge that everything you've said is correct, but I'm slightly concerned about putting the issues that arise in respect to revocation in the same bucket as Disaster Recovery.

I may be the only person in the room who thinks this, but in my head, the Gap that the study group in this particular topic is to deal with Disaster Recovery and the sort of second thing that you talked about, which is calamity in the country, et cetera.

There's a very clear distinction between those two things, which is in the case of revocation, everything you mentioned kind of arises because of the lack of cooperation from the ccTLD manager, which I get, and I understand that that is an issue. The Disaster Recovery thing that I'm thinking about is where the ccTLD manager needs your help.

I just want to make sure that we're clear what we're talking about, because I actually think those two things have distinct and separate solutions, rather than saying we'd like to try and use the

issues on revocation where we can't get to them, all the things you said, all of which could well be true, to try and deal with those with a Disaster Recovery response, which I think is actually something different, but that may just be me.

PETER KOCH Kim, do you want to respond?

KIM DAVIES Yeah. Thanks, Chris. I don't necessarily disagree with what you just said. It's not my business to say how to bifurcate the issues, but one observation I would make is that I can foresee a scenario where a Disaster Recovery response, as a consequence of the disaster, the ccTLD manager is not cooperative. Now, it might not be through their desire. They might just be fundamentally incapacitated.

So, I think that's where there's a potential nexus between, it's hard to draw clean circles around those two things. As I mentioned from the forefront, I mean, this is an expression of issues we see, but how this community wants to tackle them is for this community to decide.

PETER KOCH Thanks, Kim. And I duly noted, Chris, the remark you made, just a technical or administrative issue in that case. When we started, I said that this session and the study group were starting from two places at the same time. So, not all of what is presented here will be necessarily within the mandate of the study group, but input, of

course, can be as broad as it is, and then we will work from there. So, with no further ado, Rocio, you're next.

ROCÍO DE LA FUENTE: Thank you. This is Rocío from LACTLD, and I just wanted to mention that ccTLD regional organizations have also played a role in cases of Disaster Recovery, and I think this is an important aspect to take into account in the conversation. And even individual ccTLDs from the same region have played a role helping to restore operations in cases of natural disasters.

We have even a project that is our AnyCast Cloud, and we provide secondary service for many ccTLDs, and this is a way also of preventing this type of scenario. So, I just wanted to add that to the conversation.

PETER KOCH: Thank you very much. And then I have Jordan Carter, please.

JORDAN CARTER: Thanks, Peter. It's Jordan here, .au and the chair of the briefly lived policy Gaps analysis Working Group. I came to the same conclusion as Chris, oddly, in the scope discussion, and I thought that the way that you described the challenges of non-cooperative registries, ccTLD managers sort of summed up a policy Gap that I hadn't quite thought of, which is if there is a revocation policy as an ultimate

end stop to accountability for ccTLDs, it's not much of an end stop if it's unimplementable.

So, I wondered if it raised a different Gap, which is, if we think we know we can revoke in extreme circumstances, but actually we can't, is that a different Gap that we need to consider in those terms as opposed to the sort of natural disaster-y type of approach? That I certainly had in mind for this topic. So, just more food for thought. Thanks.

PETER KOCH: Yeah, thanks, Jordan. We'll note that and carry it maybe to the council at some point. Thanks. I think Eberhard had his hands up.

EBERHARD LISSE: I'm the chair of the Technical Working Group, which incidentally was formed after a hypothetical in Wellington at the ICANN meeting, where we went through exactly this situation. I fully agree with Chris that we shouldn't separate, that we should separate revocation as a policy decision or decision from assistance from Disaster Recovery. But the process that then follows in order to maintain stability and security of the internet is the same.

So, if we make sure that we don't mix up these two entry points, the process that IANA develops, I'm very happy with the way they handled the .LB crisis. We should separate these things out, how we get there and what we do.

PETER KOCH

Thank you very much. And with that, I see no more. Is that an old hand, Jordan? Okay, there's one more hand. And after that, we'll pause the discussion at the valuable input. I'd like to give the other presentation preference and then have a discussion later.

TOM BOLT

It's Tom Bolt from the .vi on the Virgin Islands. We have dealt with disaster time and time again. But my question is, I mean, shouldn't we be looking to preventive measures? I mean, is there a model of TLD disaster plan? Are there ways such as the placement of, if you are in a natural disaster zone, such as the U.S. Virgin Islands, I mean, we have our servers are in Vancouver, Canada. I mean, the placement of the service.

And the other issue, I think that I see with the internet and with ICANN, the second generation coming to the table. And are there succession plans that are, we see this all the time in the legal field, where there's a sole practitioner, but they have to have like a published succession plan, what will happen?

So, I mean, I think that there are preventive measures that we could be putting in place, as opposed to looking towards revocation, which is very difficult, as Kim has said, but preventive measures, I think is the way to go.

PETER KOCH

Yeah, thank you very much. I also believe this is very valuable input to the work of the study group, and would invite you to submit that or even join. With that, I would really like to go to Francisco, for a short presentation on the EBRO and escrow services. Again, this is not to advertise this as a solution. This is just one input into the whole picture. Thank you so much.

FRANCISCO ARIAS

Thank you, Peter. So, this is Francisco Arias, I work in ICANN, my team deals with gTLD technology. But I come from the ccTLD community, a long time ago, I was the head of technology in .mx. So, in the gTLD space, so this is a presentation about what we have regarding continuity of service in the gTLDs.

So, the first element you are going to find here is Data Escrow. This is a service that is critical to allow ICANN to restore registry services in case of catastrophic failure by the registry or for the matter for their risk service provider. In this sense, gTLD registries and registrars, for what it's worth, are required to escrow registration data with an ICANN approved Data Escrow agent.

So, this is a third party, there is a contract that names ICANN as, I forgot the legal term, but we are beneficiary of the data in case certain conditions are met. The registries are required to deposit daily. This registration data either has a full deposit, meaning all the data, or a differential, meaning only the difference from the previous full deposit, the previous deposit that is.

The Data Escrow deposits follow RFC, the RFCs that are noted there, that's an escrow format that was standardized in the IETF not long ago. And the registry agreements, the contracts that they have with ICANN, specify what data is required to be Escrowed in these deposits. You can find more information about the Data Escrow program that ICANN has.

Again, this is focused on the gTLD space, that's what we're focusing here. So, you can find information about what we do and what we have in there.

So, the next element that we have for this service continuity program in ICANN is, we have active monitoring of these race services. And for that we have a system, one of the most complex systems that ICANN runs. This system monitors the compliance with the SLAs for both races and registers, is based on Zabbix monitor platform, plus some custom code.

This Zabbix, for those of you that may not have heard the name, it's a company in Latvia that provides Open Source solutions for monitoring of services online. I believe they are mostly focused on financial services, but we found that to be useful for us and we have been using that platform since the previous round of gTLDs.

In order to probe the services of the registries, we have a network of approximately 40 nodes that are distributed globally. We try to place these nodes in networks where the most users are concentrated in the internet. Those nodes send the queries, DNS,

RDAP, to the race services and then the information is centralized, where it is compiled, analyzed, etcetera.

And we get the results of those calculations. We also have a network operation center that is operating obviously on a 24 by 7 basis. They are able to handle the alerts that the system triggers and they can call staff that is available also 24 by 7. We have an on-call role in my team to handle this type of issues. Next slide.

Paired with that monitoring system, we have an API. We call it the MoSAPI, Monitoring System API. This is a REST API that allows registries and registers to retrieve the information. We publish there the information from the SLAM, the condensed information from the SLAM. By the way, we also publish their information produced by our Domain Metrica program related to DNS Abuse.

And so, each TLD can see their own information. They cannot see the information from someone else, just to be clear. Now, the system that I mentioned before, where we do proactive monitoring of services, we also monitor the DNS service for all the TLDs and the root, even though ICANN doesn't have an agreement, an SLA with ccTLDs, for example, or the root. We still monitor the service.

We want to know what is going on, what is happening in case there is an issue, so that we can at least alert someone if we have the proper contacts. It's not a formal type of arrangement like in the case of the gTLDs. It's merely an information sharing type of thing.

So, that's why we have information regarding each of the ccTLDs' performance for the DNS service and the DNSSEC.

So, in case you were interested to access this API, that is something that is available, and some of you indeed have access to that API. In this slide, you can see how you can request access to that API if you are interested on accessing your information.

So, I mentioned we have Data Escrow that takes care of giving us the data we need in case of a catastrophic failure, and I mentioned the monitoring system that we use to constantly check what is the status of that service. In the contract with the gTLDs, we have what we call emergency thresholds.

These define the thresholds upon which ICANN is allowed to take the operation of the TLD on a temporary basis to restore service. And to be clear, we only do this in case we are unable to either contact the registry, the RSP, or if they don't have a solution that will guarantee a quick restoration of service. And one thing to note, even though we have an emergency threshold for EPP, we are not currently monitoring that one.

And in the case of Data Escrow, it's a little bit more complex than what it says there, but there is a simplification that we are proposing that will come in the next round raised agreement, which is a little bit more-easy to understand, so that's what I'm using here. One more clarification is I should say that when I say weak there, it's in reality the continuous seven-day period.

So, it's whatever is on the current time, seven days before, that's what we consider the window for these emergency thresholds. Next slide.

PETER KOCH Can we have the next slide?

FRANCISCO ARIAS So, while it's loading, so the last element that we have in the service continuity program, oh there you go, is what we call the Emergency Backend Registry Operator, EBERO for short. And so, once we are able to monitor proactively the gTLDs, the registry services, and we have emergency thresholds defined in their contracts that specify exactly what ICANN can do in case those thresholds are met.

We then need another element, which is this one, the EBERO. The EBEROs are providers that we contract, we have them under contract. They are ready to be activated 24 by 7, and they can be temporarily activated to take over the given gTLD, the critical functions. In the contract we define those critical functions, as you can see there, DNS, DNSSEC, EPP, RDAP, and Data Escrow. And we unfortunately, have used this EBERO element seven times in the, since we started this program with the launch of the 2012 gTLDs.

So, we have taken successfully seven gTLDs to EBERO. At the moment they are still running in the EBERO platform. We were able to restore service quite quickly. We have, in case you are interested on knowing more about those cases, I have presented about this

topic in a few sessions here in ICANN, in the CCNOTE, ccNSO Tech Day.

So, if you search for EBERO in the CCNOTE, ccNSO Tech Day archive, you're going to find that in previous meetings. And I believe that's the end of my presentation.

PETER KOCH Thank you very much, Francisco. I would like to progress to the next speaker then, which is a previous speaker, Régis, with a perspective from your TLD operations. Thank you.

RÉGIS MASSÉ Thank you, Peter. It's me again. I take another cap this time. I will talk as the CTO of AFNIC and just giving some testimony about things on Disaster Recovery, on things we see in real life. First of all, it's difficult to define disaster and recovery, but if we consider that there are some things more than natural disaster on cyber, I have tried here to make not exhaustive, I think, but a large view of threat categories about Disaster Recovery.

I think some of you have noticed the disaster South Korea has had one month ago. Big data center has 22 hours of fire that have made down some more than 1,600 government services. Hopefully, it was not the registry, but it could be. And a registry can have this kind of problems if they are hosted by a data center. During a maintenance operation, a battery, a young battery has exploded

and it takes fire. So, it can happen. It happened in France also sometimes.

So you've got disaster, you've got HR Medical things, you've got Cyber, External war tensions, geopolitical things, and financials. And I will now just share with you one kind of disaster that just have been taking place one month ago. I had the authorization of the CEO of .MG to speak about that because we know him well because he's part of the AFTIC board.

And on September 25, the .MG registry was burglarized on the night. All computers and electrical equipment were stolen, leaving no production tool in the office. So okay, the resolution DNS still works, but all the registration system and all the things of the registry were stolen. And I say here with great courage because it's a small team and they ask us some help.

We try to help them, but they have also local helps from the community in Africa. The registry team has, in five days, implemented the recovery procedures. They have SOMs, deployed a new recording infrastructure on a local ESP, and re-installed Cocca, used external backup, and restart registration.

And they say for the moment that there will be, I think, like before at the end of the year. So, for it, it's a very important problem, issue. It was very important for them. And hopefully, they had some procedures. They are aware of Disaster Recovery. And it was

not a natural disaster. It was just a geo-codable problem in the country.

And about that, just to add what Federico says just before, they had a kind of Data Escrow. They have backups and they have things outside the registry. And I think it's important because it's a way to be sure that you can start from something. Okay. So, he couldn't have some of you, I think, know the CEO of .MG. He's coming often at ICANN meetings.

He couldn't be here because of the problems they've got in the country. But I have asked him to share with you, and Peter asked me to share with you these kinds of things. It could happen. And I think we are here at the community, the ccNSO community, to help this kind of – to help the small registry, the registry, not the small one, but all the registry when we've got these kind of things.

And that's why, just about TLD-Ops, once again, all the registries on this list are not yet on the mailing list of TLD-Ops. So, if you know some of them, I know some of them. They are French islands, for example. I'm not a good example on that. But if you know some of them, we will try next year with the TLD-Ops group to contact them and proving to them that it's important to be part of this community, if they want to.

Of course, it's not a monetary and it's on, they are doing what they want about that. But I think it's important to them. And I will just share with you another thing, if I've got the time. Okay. It's not on

the slide, but I was talking about training in my first part of the presentation.

And I think training is one of the ways we have to think about to be sure that we are ready for these kinds of things. I will share with you that in France, one month ago, the French National Security Agency organized a national crisis. It was an exercise. And more than 1,050 organizations participated nationwide. It was not on the slide because we had to have the authorization of the national agency to share in international events.

So, that's why there is no slide on that. But I had the permission, of course. And there were two modes of playing. Either playing together or by organization, playing together if organizations are not used to a face with a security crisis and things like that. Or the organization could have their own process and play with their own teams. And the fun fact, that was the exercise in France took place on the day of a real national strike, which I did a little straight to the exercise.

It was easy to say our people would come to arrive to the place of the game. And it was a big stress for that. But over the course of the day, an attack scenario was deployed on the crisis unit to implement action in Rampart to inform the nation received by email. And at AFNIC, we have decided to adapt the scenario and all the messages, more than 80 messages received to the crisis unit during the day.

We have adapted all the emails to our job, to our registry procedures on our job. So, it was just to make the exercise more realistic for the players. And we are using our softwares, our employees' names and so on. So, this improved the credibility of the elements and allow the crisis units to make better tests and to take better decisions and better tests on the procedural mechanism.

So, now feedbacks are currently being compiled in order to learn from the exercise and see which element can be consolidated and improved. I will see in the next future, we don't know yet and we have to ask our government, if we can share with the community the exercise, the French exercise. And as we have adapted in ccTLD, I think maybe it could be interesting for some of you. So, I think training and education are essentials and it's very important to train your teams to this kind of things. I think it's okay for me this time.

PETER KOCH Thank you for this great insight and also many thanks in absentia to the Madagascar TLD for being open or allowing you to be open. We'll have time for one or two quick questions to Régis, but before we do that, I'll give you a head warning. There will be an interactive part with questions on Mentimeter after that, so if you haven't already, get out your mobile phones or your laptops and go to menti.com and after that you get either the QR code or here you go. So, are there questions to Régis? I see Eberhard.

EBERHARD LISSE: We also run CoCCA and we run it in a DAAR. We run the hardware, not on a virtual machine, on iron in Europe in the data center in Germany, Knipp Medien. They also run ironDNS. They also are a backend provider for a couple of registries with Core, I think. That means their infrastructure is so that they have automatic failure into another data center.

That said, we still automatically backup the data every hour on the same machine and every two to three hours onto a different machine outside of the country, outside of the continent. And never mind replication, but if our hardware fails, we have a standby machine in the data center that comes up with the rate that you pull out and pull in. So, even for small ccTLDs, having an idea what to do if these things happen would have sped up .MG's recovery by a few hours.

The point is, does it really matter whether it's a few hours or a few days as long as the DNS is not affected? You cannot renew, you cannot register, and you cannot delete. So, that works. My question that I have actually was to Francisco. How does, when a TLD goes into EBERO, how does the DNSSEC work? Because then you need a new DS key in the root and how does that work?

PETER KOCH: So, I'm sorry to intervene. That's a very interesting technical question. I suggest we postpone that for discussion because we

really want to go through these questions and I fear we get too technical if we continue here. Apologies for that. So, the prep team has, what a prep team does, prepared some questions here. So, if you go to Menti, we would start some questions.

Well, the initial question, do you work or represent a ccTLD? That is great, so that you get yourself familiarized with that. We welcome guests, but we also ask, when we ask about is this a ccTLD perspective, that only people who have that relation to a ccTLD respond. It doesn't matter how many people from a ccTLD there are, but it would be great if we could respect that suggestion. Thank you so much. So, with that, that means we have at least five people in the room from the non-ccTLD part of the world, which is great. Welcome.

Next question. Does your TLD, that is ccTLD, have a Disaster Recovery or continuity plan in place? All right, that's great. Roelof is confused.

ROELOF MEIJER Yes, very much, because it seems that the responses are all over the columns. You would expect the yes to be blue and the no to be red or something, but you would expect the yes to be blue and yellow and red at the same time.

PETER KOCH So, can the secretariat clarify?

ROELOF MEIJER Or at least that's the cause of my confusion. If I'm the only one, just ignore me.

PETER KOCH No, I share that confusion. Could the secretariat clarify what the color codes mean? Is that taking into account the response to the previous question? Okay, perfect. So, I wasn't as confused as I thought. Right, so that includes the high number of yeses and the noes and the people who voted unknown in the first question.

So, that's an impressive 81%. Also, the prep team is happy that we see this. I would have to ask the right people, because we were discussing about the value of those separations. But anyway, we can conclude here there is a high number.

Does anyone have any verbal addition to provide to whatever they voted for or whatever they chose? Now I get my fourth pillar here. Any verbal intervention? No? Okay, then let's move on to the next question.

Please indicate your level of agreement with the statement below. And the statement is, my TLD is able to recover its operation after disaster within 24 hours. And the gut feeling is okay, of course. That is again a good 80% four out of the scale of five. Okay, it is probably slightly lower. It is slightly lower from what we saw before from those who had a plan in place.

Luckily, the confidence isn't so high that it would increase the people that do not have a plan, right? That's also a message, even though we don't know how these correlate. Okay, thank you very much. We'll take these inputs. Anyone want to make a statement on what they picked and why? No? That's okay. Then let's have the next question, please.

EBERHARD LISSE Sorry, I have a small question.

PETER KOCH Absolutely.

EBERHARD LISSE Next time, don't make such a slider because that could be skewed by if there is a few with one and a few with five that averages out to something which is not what we actually expect. So, you need to have columns there as well, I think.

PETER KOCH What you say is very correct. But this is all about temperatures of the room, right? This is not a scientific exercise. We'll take that into account when we deal with the numbers. But thank you, you're right on that point.

So, which part of your operations is most vulnerable in a crisis situation? Select all that apply, and then there's the number underneath. DNS resolution seems to be strong. Don't know is fair.

Legal and governmental interference. This is an interesting crowd, I must say. And the registry system, key management. Does anybody want to speak on other? You can remain anonymous, I think.

ROELOF MEIJER Can I? I'm sorry.

PETER KOCH Yeah, no, go ahead. This is Roelof, by the way.

ROELOF MEIJER Sorry, this is Roelof Meijer, .nl. DNS resolution, registry systems, DNS key management, legal contractor, organizational continuity, those are all operations. So, how is the legal or governmental interference meant? Because that seems to be not an operation, but an interference.

PETER KOCH

Yeah, and the more interesting it is that so many people picked it. What we what we yes, that again, the phrasing is probably a bit imprecise, and I sincerely apologize for that. What we meant is, in that case, the interference isn't vulnerable, but the whole system might be vulnerable by being interfered with from whatever government or regulatory interventions, I guess.

I hope people read it that way, because that is the way the PrEP team came up with it. Thanks. That gives an interesting picture. Any other questions or does anyone want to share what their perspective was and why they have that perspective? No? You all want to stay in the masses here. That's fair. Okay, I think we have another one, don't we? Yes, here we are.

In one word, and that's a word cloud to be, in one word, what's your biggest concern when it comes to continuity of your ccTLD? People are typing long words. Just the author of the or whatever the lab, the bird lover, would the bird lover explain the intervention? The black swan? Yeah. I know it's too ahead.

ROELOF MEIJER

Yeah, a black swan is a completely unexpected thing. Something you've never thought before until it happens.

PETER KOCH

Yes, perfect. Thank you. Okay, now we stabilize or not. Okay, thanks. I think we can take it from here. This is a very nice result or not, but centering on geopolitics, given all the work that we

collectively do in the worldwide internet governance. That's a nice bottom line here, I guess. Thank you so much. I think that was the last one. Do we have one more?

CLAUDIA RUIZ We have two more.

PETER KOCH Oh, we have two more. Wow. Then imagine your ccTLD went down tomorrow. How could AINA best help you? Catching the black swan, of course. Okay. Thank you very much. It looks a bit like we are approaching the end of the day, actually. Let's take these into account. Does anybody want to elaborate on one of those? No. Then let's have our final question for the day or for this session. Please.

What is the one thing you wish your ccTLD had in place today to improve disaster preparedness? The one thing. Small escrow and large Escrow. That is one dish. Give me two more. One. And finally. Great. Thank you very much. With that, we can close this part. We'll take this as input into the study group. Thanks for actively participating in this. This is very important and I hope it's a bit of fun for you.

Preparing at least made fun. And how would you this session? We're not done yet. It remains for me to thank Kim Davies, Francisco Arias, Régis Massé, for the contributions, the prep team for setting up the session, the secretariat and AV staff for making

this technically possible and smooth, and also the members of the study group for input. If you are not curious what the study group is and may be interested in joining, there is still an opportunity to do that.

If you want details and want to learn about the mandate and what potential work commitment would be, please talk to the secretariat or myself or any of the council members. We can help you with that. Volunteers, welcome. And with that, I'd like to thank you all and close the session. The session is adjourned.

[END OF TRANSCRIPTION]