ICANN86 Seville | PF – ccNSO: Regulatory Trends on DNS Resilience Affecting ccTLDs (1 of 2)
Tuesday, June 09, 2026 – 14:45 to 16:00 CEST

CLAUDIA RUIZ

Hello, and welcome to the ccNSO Regulatory Trends on DNS Resilience Affecting ccTLDs 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 Community 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. 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, and please speak at a reasonable pace to allow for accurate interpretation. Thank you. And with that, I will now hand the floor over to Annaliese Williams, moderator for this session. Thank you.

ANNALIESE WILLIAMS

Thank you, Claudia, and good afternoon, everybody. Thank you for joining us. My name is Annaliese Williams from the .au ccTLD, and I'm also the chair of the Internet Governance Liaison Committee. This session is a collaborative effort between three groups within the ccNSO that consider the theme of resilience from different perspectives. So it's been a collaboration between the Internet Governance Liaison Committee, TLD Ops, and the study group on the role of IANA in ccTLD disaster recovery. And we have the chairs of those groups here as well. So we have Peter, and Reggie is over there as well. So thank you.

So this session will explore global regulatory developments relating to DNS resilience and the impact on ccTLDs. And there's two parts to today's session. Part one features some guest speakers who are joining me here up at the front, sharing their insights on this topic. So we have Dan York, the senior director for online trust and safety at ISOC, Elena Plexida from ICANN, the vice president for government and IGO engagement, Dimitris Zacharias, also from ICANN, senior manager for government and IGO relations, and Maarten Aertsen, who's a senior Internet technologist at NLnet Labs and also a member of the SSAC. And then after the break, we will be hearing from two ccNSO members who'll be sharing their perspectives. So yeah, it is a two-part session. So we'll finish up with a brief overview of how the various groups in the ccNSO are addressing the broader theme of resilience. So I'd just like to remind all of our speakers to speak slowly and clearly. This session does have interpretation, so please

make sure that you have a headset handy. And we will also be using Mentimeter a bit later, so just a heads-up on that. Have your phones ready to participate in that. So I will hand over now. I think, Dan, you'll go first. Each of our speakers has about 15 minutes, and that includes time for questions afterwards. And so I'll hand over to you, Dan, to tell us about cybersecurity regulation.

DAN YORK

Hello. Thank you all for coming here to talk about Internet resilience. This has been a topic, obviously, it's been a theme at recent ICANN events and beyond that. At the Internet Society, we're obviously focused around Internet resilience as one of the pieces that we do. We do a lot of time measuring it, looking at it, adapting it. For this particular session, I was asked to give a bit of a global view around what do we see across the world in terms of regulations, in particular, that are around Internet resilience and critical infrastructure and pieces like that. Let me just have a quick show of hands. In how many countries, in your countries, is Internet resilience part of a government legislation already? Yeah. Good number of folks around there, all around the space.

What we've seen, if we can get my slides up, please, is that we're seeing now that DNS was once just kind of something that happened. It was part of the Internet. It was part of the things that were there. And it was... Oh, I'm supposed to push the button. Sorry. There we go. Perfect. There we go. Okay. DNS was plumbing, right? It was there. It just worked. That's what people thought. It

was all great, and it was just there. But now it is becoming critical infrastructure. And if you know anything about the phrasing of that, when you start talking critical infrastructure, you're starting to talk about a space where governments get involved in some kind of range around that. But DNS, as we are all here, is really the backbone for so much of what we do in our digital economy and our online world around this. A couple of years back, this kind of conversation around DNS as critical infrastructure, a lot of that was happening here in the EU, where we are today. But now it's happening everywhere. If we look at the range and what's going on is you're seeing that technical coordination is really becoming regulatory oversight. My colleagues to my left and right will be talking about the EU elements around that shortly, but it's not just here. You can see this long list that's up on the slides right now. There's legislation in the UK, in the US, China, India, Australia, Singapore, Saudi Arabia, Zambia. It's kind of everywhere. There is different legislation that affects the resilience of the DNS and of the Internet in general around.

So let's look a little bit about why this is happening. Certainly, we're seeing a lot of increasing attacks that are going on that are targeting infrastructure in different ways, whether they're extremely large-scale DDoS attacks, whether they're other pieces around there. There is this dependence that we're all used to at this point, where Internet connectivity, the ability to do services is just woven into the fabric of our lives. And we're seeing that national security elements, economic stability, because we have been

successful as an industry with having the Internet become part of our lives, it is now we are dependent upon it. So when the Internet goes down, as this part of the world saw just two years ago or so, these things have serious impacts that just affect our ability to do pretty much anything and what we are. And digital security, it's a political issue. Governments are looking at all of this. ccTLDs are also an interesting intersection because they're regulated entities, but you're also critical to the resilience of what goes on in so many ways.

So if we look overall at the trends that you can sort of pull out of all of these different regulations that you could see, I've identified five of them here, and I'll walk through each one in a little bit, but operational resilience, incident reporting, data governance, baselines, and then supply chain. So the piece with resilience in general is that it's not just... Regulators are now naming DNS specifically as part of critical infrastructure. At some times, Internet or information technology is a part of it, but DNS is now specifically being named. That's part of one of the changes that we're seeing. There are risk management requirements in some of these different regulations that are out there. There are business continuity expectations. There are requirements being put onto DNS infrastructure around what it should be up, all these different kinds of things around that. Another piece is incident reporting, and this is certainly one of the big ones, ranging from six hours to 72 hours, depending upon which regulation and which country is out there. But it's saying this, that you have to rapidly report when

there's any kind of outage, usually to a government agency. There are mandatory disclosure. It's not just one of these things of, "We'll handle it quietly," or, "It was just a bump. We'll fix it. It's all back up. It's all good." No. Any kind of outage is being mandated to be reported in some way in some of these legislations that are there. There's also an interesting aspect that many of these regulations are adding in executive accountability and liability. People can either be fined, executives of an organization can be fined or can be put to jail or whatever the type of element for the breach of this kind of incident reporting. If you don't report it, you could be fined. Looking at different, again, across the world, different regulations are looking at different ways to do it. Carrot, stick, both, all of those different kinds of things around that. Every new framework that we're seeing usually has some level of incident reporting as part of it.

We're also seeing, of course, greater interest in data governance, data sovereignty, data autonomy, pick your word. There's a lot of interest of how do we wind up having more control over what's in our region, what's in our area. We're seeing also, again, a resurgence of law enforcement access requirements, which have always been there, but we're seeing a lot more of that now. Aggressive takedown mandates that we're seeing, some very quickly. There was one not too long ago in Italy, the Piracy Shield, where I think the one IP address blocked about 300-plus domains. There's these kind of things that are happening out there. GDPR, things around this foreign control, kill switch discussions that are

popping up in different areas. The pressure is on in looking at how do we take care of these kind of things. The fourth trend is just what we used to say were the kind of voluntary frameworks that you would sign up to. You'd say, "I will adopt these norms," or, "We'll do this." Those voluntary frameworks many times are now becoming what is the regulated requirement. So, whether it's defining the base level expectations around this, lifecycle vulnerability, ensuring that it's all being tracked. All of this is important pieces.

Which brings us to the fifth one, and I was just actually reading news this morning around yet another supply chain attack where someone had gone and compromised a whole series of Microsoft's software in a GitHub repository. But that was then being pulled out by many of the people that were using it for, in this case, it was AI agent usage. But still, regardless, it was being supply chain elements over there. Maarten will talk to us a little bit later at some length about where he sees this as a software vendor in some form. But for you all as ccTLDs, these requirements are now causing... You're responsible for not just your own security, but for the vendors, for the software that you use in some form. Whether that is, as I put on the thing here, whether it's your DNS software, it's your providers, anything of this can be in scope depending upon where you're located, what is there, all of those kinds of things. A challenge around this, of course, is that you might be subject to multiple different kinds of regulations. You might have national

legislation, you might have regional legislation, all depending upon where you are in the world and that.

I think for you all, and for all of us who are involved in this kind of space, the implications are pretty clear. We're being classed as critical infrastructure. We have to be thinking about that in some way. There is this tension, as I talked about, between global, regional, national legislation. You might have multiple different kinds of reporting requirements, disclosure requirements, agencies you must be talking with. For some, depending on the size of your ccTLD in particular, this could be quite significant in what kind of resources you might need to have to go and comply with all of that. And the supply chain piece is, I think, a big one because you need to understand all of the software that you use, the systems that they're using, the Internet connectivity, the ways all of that is potentially there. I will say, though, that there is this opportunity because you are being classed as critical infrastructure, because that's there, I think there is an opportunity that you can engage with some of those discussions around there because you are now part of that. I think there's also a good suggestion that there's opportunities to work at the more regional level, to look at how do ccTLDs work together to go and do that. So I will leave with just two questions for all of you to think about, which is one is, do your government cybersecurity regulators know who you are? Do they know what a ccTLD is? In some parts they may, other parts they may not. And is your ccTLD in scope of one or more of these

regulations, and do you know what that means? I would leave it with that and pass it on to my colleagues to talk about EU.

ANNALIESE WILLIAMS: Thanks, Dan. I'm not sure who we... If we're going Elena? Okay, thank you.

ELENA PLEXIDA: Thank you so much, Annaliese. Hello, everyone. Dan gave us the global trends, and my colleague Dimitris is going to talk to specifics with respect to EU legislation. Europe continues to be the most consequential jurisdiction in terms of legislative initiatives for the DNS ecosystem, so there's a lot of attention there. Now, that said, they make my life very easy because I don't have that much to say, at least at this stage of the conversation. I have lots of opinions for later on.

So for now, let me just say this. This community is all about resilience. The stable, secure operation of the DNS is the very reason why we're all here. It is a big deal for us. It is the deal for us. It has been the big deal for us way before it became a policy issue or top of agenda for the policymakers, of course. ccTLDs are a unique part of the community, as they are equally unique for their countries. Right. Now, we do have, in the broader DNS cybersecurity ecosystem, if I can put it that way, we do have, of course, some security-related obligations for gTLDs, such as data escrow or registry system security requirements. We have tech DNS

standards such as DNSSEC by the IETF. We have industry best practices, and here the ccTLDs lead. And increasingly more, as Dan walked us through the global trends, we now have regulation. Many countries view their ccTLDs as critical infrastructure, as Dan said. Some countries further view other DNS operators as critical infrastructure as well. So we have specific cybersecurity requirements and incident reporting obligations by law here. I would say that these different pieces synthesize the DNS cybersecurity landscape today.

ICANN follows all these legislative developments to the extent that we can. Of course, we're not everywhere. As you know, we do follow that. Now, what's our angle? First of all, importantly, as Dan again said, DNS is specifically called out now in these legislative pieces. Our angle is the community work and the multi-stakeholder model. So is there community work that could be affected by legislation? Is there community work or community initiatives that policymakers should be aware of to inform the policymaking? Is any legislative initiative going to impact in any way the multi-stakeholder model's ability to maintain the global coordination that the multi-stakeholder model ensures? That is the ICANN organization viewpoint when we follow these kind of things. And as I said before, ccTLDs are unique. Everything is interconnected, though. It's like communicating vessels. ccTLDs are on the ground. They are the first to feel and understand much faster the trends. So from an org standpoint, as we follow these developments, we need the cc's viewpoint, and even more so if something comes up that

we collectively think might require engagement. So there needs to be coordination there in that viewpoint. That's all from me. Annaliese, with your permission, can I give it over to Dimitris?

DIMITRIS ZACHARIAS

Perfect. Thank you. Can you hear me? Yeah. Great. Thank you, Elena. Thank you, Dan. I'll just move it back a little bit, Karla. Sorry. Yeah, good. So, thank you very much. I will try to go into a little bit more detail about the pieces of legislation that Dan and Elena both discussed. I'll try also to not go into too much detail, so if there is something that you pick up that you find interesting, we can also discuss in more detail further so that I don't tire you with article numbers and paragraphs of provisions of EU law.

So for those of you who are not aware of the details of the NIS2 Directive, this is a very short introduction. The reason why this is very important to use as the foundation for our conversation today is because the NIS2 Directive, building on the original NIS1 Directive, is essentially the platform on which further sectoral legislation in the EU in terms of cybersecurity will be built on. And why is this important for the space and ccTLDs? Because as Dan mentioned before, ccTLDs, and generally the DNS, are part of critical infrastructure. So knowing that in the future more legislation will be founded on the way that entities and sectors are classified based on NIS2, we can expect that future initiatives will also potentially include the DNS and ccTLDs within their scope.

So what really is the NIS2 Directive? Of course, at a time of heightened cyber threats in the EU, there was a renewed interest for a cybersecurity strategy. And based on that, of course, the member states' capabilities to fend off attacks and increase the resilience of network and information systems. The NIS2 Directive is built on three blocks. The first one is a scoping exercise. Which sectors, and from which sectors, what entities would be falling within the scope? Once an entity and a sector are in scope, those entities identified will have to adopt certain cybersecurity risk management measures, which are very detailed. And as Dan mentioned, it can start from incident handling to business continuity, to cyber hygiene and training, all the way to MFA and cryptography. So there is a broad range of cybersecurity requirements within the pieces of legislation, and all of the entities need to comply with those. Once those measures are in, then the third block is the reporting of incidents. The European Commission and the member states figured out that there is a lot of information flying around at the national level between ccTLDs, if there is something happening there, and the competent authorities. And with this piece of legislation, they try to formalize not only the timeline, but also the information that is shared between a party that has undergone some kind of a risk or attack with the corresponding national competent authority. So all of those things were formalized. We're talking about a three-step incident reporting process. And of course, there was an implementing regulation right after NIS2 was adopted to specify what a

significant incident is for TLD registries and for a lot of other entities included within the scope.

This is a key point here. The NIS2 Directive, for those, again, not aware, directive means that there is a certain leeway in adopting it or downloading it, if I may use that term, from the EU level to the national level. There is a certain degree of freedom where national administrations can take additional steps or decide to implement in their own way. So in order to ensure some kind of alignment, the European Commission also came up with an implementing act to specify what a significant incident is and to build a menu of cybersecurity risk management measures that entities can adopt. Why is this important? Because very recently, in the new cybersecurity package, which was revealed in the beginning of this year, there were already some targeted amendments to the NIS2 Directive. Mind you, the directive has been implemented in 23 out of the 27 member states of the EU, and it has been a very long process in getting that done. We can discuss if there are any questions about the lags of the implementation at the national level. But for the purposes of our conversation, there are already some changes that are happening to the NIS2 Directive, mostly when it comes to the scope. What the national administrations understood is that there are way too many entities for the national administrations and the authorities to be able to ensure compliance and enforcement. So there have been some changes into the scope. Some entities are now being treated as important entities, so it's only ex-post enforcement of those provisions. And

there have also been some other steps, the most important of which is a maximum harmonization for cybersecurity risk management measures. As I said before, NIS2 is a directive, so there is a certain degree of freedom. But with this change, when it comes to cybersecurity risk management measures, member states cannot do more than what is prescribed centrally from the European Commission at the EU level. And again, that is in an effort to kind of simplify and harmonize across 27 member states.

Together with the amendments to the NIS2 Directive, our building block for today, we also have a new Cybersecurity Act. As Dan mentioned before, the European regulator is trying to codify a way in which to assess and address risks stemming from the supply chain. The package was revealed again in the beginning of the year, and it's essentially a way in which the European Commission is building a trusted supply chain framework, working on modernizing and making more effective the certification process, which hasn't really worked great so far in terms of the timeline, and also to strengthen the EU strategic autonomy in some of those critical sectors and technologies. Those are the three pillars of the Cybersecurity Act. I'll let you take a look at it, but in order to economize a little bit on time, I will move on to what would be the impact of all of this entire package on ccTLDs. So, as Dan mentioned before, ccTLDs are now part of the team that comprises critical infrastructure. You may hear it as digital infrastructure in some pieces of law, critical entities in some others, but this is essentially a key change. And the second thing is that because the

DNS is part of the core network functions of fixed and mobile electronic communications networks, this is de facto classified as a key ICT asset in the supply chain framework. So that means that for this space, the supply chain provisions that will come out of the negotiating process will also be not only relevant but also implementable.

I would like to talk about another and final piece of legislation that is on our map, if I may say so, and I know that Maarten will later on delve into more detail on that. But that is the Cyber Resilience Act. And why is the Cyber Resilience Act important for the space? Because every software and hardware product with digital elements that is placed on the EU market needs to undergo certain processes to secure security by design, certain processes for patching vulnerabilities and reporting those vulnerabilities, and obtaining a CE marking, which is something new that the commission also, and member states, agreed upon during the negotiation process, and that is to demonstrate and attest compliance of those products for entering the EU market. Now, there's a bunch of obligations stemming from the Cyber Resilience Act. However, those are not particularly applicable to ccTLDs. What would be applicable to ccTLDs is considering two things. First, the operation of the registry largely NIS2 serves as a foundation. If the registry has developed or commercialized software products for third parties, then those could potentially fall under the CRA. So there will be a slew of requirements that would also stem from that piece of legislation onto potential software products. And the other

thing is the supply chain security and reporting ecosystem. If there is a way in which registries or their products would fall within the scope of the CRA, there is another wave of requirements that would stem from the Cyber Resilience Act.

Before passing on to Maarten, I would also like to take a second in case you've been seeing in the news that the European Commission also proposed a tech sovereignty package earlier this month, about a week ago, if I'm not mistaken. It's comprised of two pieces of legislation and a communication: Cloud and AI Development Act, Chips 2.0, which is a way for the EU to build more capacity in sourcing materials and producing semiconductors, and the open source strategy, which I know Maarten will speak a little bit more about, including some more information on the CRA and the open source software community. Thank you very much. And with that, I would pass on to Maarten directly, or?

ANNALIESE WILLIAMS: Yes. So just to let everybody know, we are planning an interactive session today, so there will be an opportunity for you to ask questions of all of the panelists and engage in some discussion with questions that might be put to you as well. But first we'll pass to Maarten, and then go ahead. Thanks.

MAARTEN AERTSEN: Thanks for having me, Annaliese, ccNSO. So I work for the NLnet Labs Foundation, a nonprofit based in Amsterdam, the

Netherlands. And at NLnet Labs, we work on open standards in the DNS and in routing security and their implementation in software, which we license, which means you can freely use it, you can study it, you can change it, and you can share it for any purpose. So today I'll share our perspective on the waves of EU regulation that started a couple of years ago.

So my role at NLnet Labs, unlike that of my colleagues, who are either software engineers or researchers, is to work with policymakers. So as an organization, most of our efforts go into developing and securing software, and that's what we've been doing for decades. But that's not what we will talk about in this presentation. We'll talk about the policy side of things. And that's at times a bit uncomfortable. Perhaps you recognize this in your registry, how practical efforts to keep things secure may sometimes be disconnected from the efforts you go through to comply with legislation, even if the goal of that legislation is, in the end, security. But as we have, as an organization, expertise in routing and DNS, I try to bridge this gap and bring our knowledge to policy development processes, and that includes some of the very regulations that Dan, Elena, and Dimitris just talked about.

In the ICANN space, I spend some of my time volunteering as a member of SSAC, and I'll bring a single slide to this talk here, which was from research we did last year. If it shows. Maybe we are on the wrong deck. Yes. Great. So SSAC looked at software run by registries, resolvers, and name servers at ccTLDs and at the root. And the key finding of this report, published in October, was that

the DNS is built and sustained on free and open-source software. If you're inclined to read the full report, this is the QR code. But just to take another quote from the abstract, "Open source software is not inherently more or less secure." And that's kind of relevant when we're talking resilience, right? So the security of any software project is determined by the quality of its development and maintenance processes, not the visibility of the source code. So this is where I'll switch back hats, because I'm talking on behalf of, well, my employer and not on behalf of SSAC for the remainder of the presentation.

So when we discuss resilience, disaster recovery, or regulatory interaction, the takeaway I would offer is to explicitly consider that you are using open source software as part of that equation. So if your organizations have discussions at a board level, it may feel like a detail, but I think it is increasingly not. Because in a practical sense, open source software has a different risk profile. We saw that it's not inherently more or less secure, and unlike with physical goods or with proprietary software, using it does not automatically give your organization a relationship to work with if anything goes wrong. And if your organization is focused on procurement as the key moment to determine a budget or evaluate risk, then all those dependencies may be flying under the radar. Now, we were going to discuss regulation, not how you approach things. If you look at digital regulation, the EU is at least starting to become aware of the role of free and open-source software, and so it's starting to treat it differently. And so as a ccTLD operator, those supplying open

source software to you may be treated very differently in the regulatory sense than those, for example, supplying data center space. So I'll try to zoom in later and give you a specific example. Maybe that'll make it a little bit more real.

Now, why is open source software specifically relevant? It is because the intuitions that people hold in a supply chain may not hold in this space. Perhaps these are your intuitions as a registry, but more often, these are the intuitions of policymakers or regulators in your jurisdiction. So in the presentation that Luis Diego of the Namibian registry delivered yesterday during Tech Day, there was a nice illustration of what a modern software stack can look like, and it was a picture of layers upon layers of open source software. He also pitched that such a stack has a cost-free availability, it has an absence of licensing cost for the operator, and all of that is true. However, it also means that unlike a regular supplier, you either build in-house expertise, or you maintain a relationship with who's providing this, or you silently usually accept the risk that you do not control the outcome. And this is the case for most open source software out there. So the DNS space is pretty exceptional in the sense that there are actually legal entities like organizations that you can work with and contract to care for the software in a financial sense, but also in a contractual sense, like having a place to go with issues. But for the rest of the stack, and that's what's on the slide, that maintainer is not your supplier. So this was Thomas Depierre who coined this notion in a blog post a couple of years back. And I'm making this point in the context of

this talk because the distinction where there's no legal entity is applicable to most of the software, including that which you run.

So now let's talk about actual regulation and how it affects us at NLnet Labs with an example. So it's a European example. I'm sorry. We are based in Amsterdam. I hope it's still useful. So this is 2026, and we're in the EU. And we make a piece of software called NSD. It's a secondary name server we have developed and maintained since 2001, and many of you use this directly or indirectly, for example, in an anycast DNS deployment. So I'll talk you through the various specific regulations that were mentioned by previous speakers and how they may impact here. So our publication of NSD from September 11 of this year will have obligations under the CRA. So we are under obligations that are for a so-called open source software steward, and this is a new legal construct specifically created to capture organizations like us, nonprofits, within the CRA's regulatory framework. So we cannot CE mark our software because we're not a commercial manufacturer, but we have obligations. So at the same time, the creation of this steward notion helped the legislators that were making this legislation to get most of the rest of the open source community out of the scope of this law. And if you want a specific example, for example, Dnsmasq, the software most commonly in cable modems, et cetera, is an example of not commercial software, which is still everywhere. Now, our first obligation from September 11 of this year will be to report vulnerability exploitation to ENISA and to our national CSIRT. Now, I'll share a personal observation. I've worked

at a CSIRT, and I'm a little bit critical to the practical usefulness of this obligation, but we will follow it, and we'll see how it goes. That's, I guess, also neither here nor there. From December 2027, that's next year, the remainder of our obligations will activate, including obligations to cooperate with market surveillance authorities, et cetera.

So I said we're not being regulated as a manufacturer, and you see here how the EU has specifically crafted its product security legislation to recognize that some of the entities in the DNS space act differently. It's obviously not tailored to DNS specifically, but to entities such as these. And this is the result of two and a half years of working with the commission, with the parliament, and the council to actually change this. And this is why I'm saying this is not an implementation detail. This is what matters in all of your stacks, to keep your eyes open when regulatory developments like this happen. Now, this is on the left side. It's us. Now let's talk about some of you. Let's say you or the DNS operator your registry contracts with uses NSD to provide, say, a DNS service. One of the engineers downloads NSD. Now, in Europe, this use is regulated under NIS2, and it comes with supply chain obligations. Dimitris shared some of this, right? So in particular, the NIS2 Implementing Act gives responsibilities to assess indirect supply chain-related security vulnerabilities, including the need to diversify and address vendor lock-in. Now, the crux of the matter is that these obligations on the left side and on the right side do not actually fully align. So we have obligations on one side, you have obligations on the other

side, and this is so because NIS2 predates the nuanced debate on FOSS. It came earlier. And so NIS2 does not actually define the notion of a supplier or what it is to be a direct supplier. Now, the most logical implementation here is to say that you're only a direct supplier if there is a contract. I'm sorry. Thank you for... I have a nice sequence of steps, and you need to press the green button to actually show them. So, thank you, Dan. So your use comes with supply chain obligations, but NIS2 doesn't actually define direct suppliers. And so here, the obligations that NIS2 sets would pass down if you outsource this DNS service, but it would not pass down to us necessarily. But because this definition is not spelled out anywhere, and this is pretty fundamental, that's not great. So we talked to the commission about this specifically, and I'll get back to it.

Now, finally, there's also the case where a ccTLD contracts for support with us or with anyone else, right? And then the situation changes, because if you have a contract for, say, technical support, there is a supplier relation, and for that relation some of these responsibilities may attach. Sadly, these types of relationships are a fraction of the total use, including in the ccTLD space. So if we're talking resilience, disaster recovery, I guess there are some observations here. We talked to the European Commission, and things are slowly changing. So ENISA, which is the European Network and Information Security Agency, in their technical implementation guidance on NIS2, says they actually define direct supplier. What does it mean when you talk about open source

software? And they're saying, basically, when there's no contract, there's no supplier. Kind of obvious. When there is a contract with a steward, this is also not what is intended with the notion of direct supplier. So this is not the actual law, it's the explanation by ENISA. And I'm quite happy that they clarified this because this is what you need in practice, right? To know where is this boundary, how does this work? Unfortunately, this nuance did not carry over to new policy proposals that have been made since. So, for example, Dimitris talked about the Cybersecurity Act, the update, and the nuance, again, is missing, even though it builds upon NIS2. And more importantly, it's no longer direct suppliers. The wording is all stages upstream. So that's basically everyone, including volunteers and stuff. So I guess our work here is not yet done. And I would appreciate if we can work together on this, because I think none of this is an implementation detail anymore. Let's see. My final slide, and it relates to the package that was presented last Wednesday. And it's just to underline that open source is not that implementation detail. Because this tech sovereignty package turned out to include an open-source strategy, which I think is at least a political signal that this is not something for the nerds anymore. And I'll leave you with that observation, and I'm hoping we can have a discussion, maybe some questions, and I'll give it back to Annaliese. Thank you.

ANNALIESE WILLIAMS Thank you, Maarten. Can I just have the clicker? I think we are going to... I'm not sure what happened then. Do we have the Mentimeter

code? Yes, here we go. So yeah, if there are questions, please scan the code and put them through. Questions to any of the panelists or questions that you would like to discuss. Are there any questions? Otherwise, Dan, I might invite you to put your... You had some questions at the start. We might put those back to the audience while people are thinking about and typing their questions. I'm not sure if we can get that slide back, but I can...

DAN YORK

Well, one question was for folks who are out there, do your government's cybersecurity regulations know you exist? Are you in connection with them? Show of hands. How many yes? How many don't know? That's good. All right.

MAARTEN AERTSEN

I have one, like as a follow-up while we're raising hands. How many of you know that organizations like mine exist? And put your hand down if you aren't sure, if you use software like us. Okay.

DAN YORK

How many of you know if you use Maarten's software?

ANNALIESE WILLIAMS

So we have had a few questions come in. I'll read out. I'm not sure who wants to answer this one, but the question is, shouldn't we speak of autonomy instead of sovereignty? Does anyone want to handle that one?

DAN YORK

I was just looking for somebody in this room who I might know who might be asking that question. So this comes about when we talk about digital autonomy, kind of control ownership. Digital sovereignty has become such a loaded term in so many different uses in different places. So I think the answer is, sure, we can talk about it in terms of digital autonomy and think about it in that form, but the reality is the larger media, the larger space, the policy environments are increasingly using that term digital sovereignty. But the challenge is that it's used in so many different ways. For some people, it's referring to the sovereignty over control over all of your resources and spectrum and pieces inside of your country. For other people, it is actually talking about personal digital sovereignty and sovereignty over the control of and usage of your own systems there. For others, it's being used in widely different forms. So the term itself, kind of like cloud in some ways, is being massively used in many different forms. So we want to be a little bit more precise and talk about control of our own systems, control of our own usage of that type of thing. Digital autonomy is another one. If you were here, or actually if you were at the ALAC session earlier, Hisham from RIPE NCC had a great presentation this morning. He was talking about, and I think he'll be talking at the Europe space tomorrow or on Thursday, around this whole topic of digital sovereignty, autonomy, and all those pieces that are there. Anyone else?

ELENA PLEXIDA

Thank you, Dan. I'll take the opportunity to stress something. I think that also goes to another question that we have there. If we can talk about resilience instead of talking about sovereignty. As Dan said, digital sovereignty as a term, or tech sovereignty or whatever we call it lately, has become super loaded. There's no definition about it, which I don't know if it's a good thing or a bad thing. I'm not going to qualify that. What I want to say, though, is that so far, the political debates at the global level, and it is a different debate in different regions, doesn't include us in the sense of it doesn't include this layer of the Internet, if I can put it that way. It's about cloud, it's about AI, it's about chips, these kind of things. This is a good thing, and we should be mindful of that and try to keep it that way. So my point here is, if they want to talk about it in terms of digital sovereignty, fine. I don't think we should try to insert our terminology in their terminology. By all means, avoid that political discussion that is about something else includes this layer of the Internet, if you will. So it would be great if we call our stuff resilience, and they call their stuff digital sovereignty, if I make any sense. Thank you.

ANNALIESE WILLIAMS

Thanks, Elena. And we have one on the screen. Do these requirements lead to any new support contract details? I'm not sure what requirements when that question came in. Did you want to take that one, Maarten? Yep.

MAARTEN AERTSEN: So I'm guessing that this question asks about the requirements from the CRA or NIS2 with respect to support contracts on software. So yeah, for each of these laws, we need to check if what we are doing is still allowed or if you need anything else. So, it's hard to answer such a general question, but yeah, come talk to me after if you have a specific scenario in mind, I guess.

ANNALIESE WILLIAMS: Thanks, Maarten. Yoko, are you going to the next question, or am I driving this?

YOKO: Apologies, Annaliese. I did not understand.

ANNALIESE WILLIAMS: Are you able to skip to the next question?

YOKO: Sure. Thank you.

ANNALIESE WILLIAMS: Yep.

DAN YORK: While we're waiting, I see one in the queue that said, "Is this affecting ccTLDs only or gTLDs as well?" It affects anyone running

DNS infrastructure. So we're in the ccNSO, we're talking about this, and also cc's have that issue that you're probably connected to some national regulator, and you may have different things in your area as well. But basically, anybody running DNS infrastructure in some form comes into this.

ANNALIESE WILLIAMS I think that one there is... Yes, we did the sovereignty. So I think we can scroll to the... So this one is, where do you anticipate directives and policies going, whether it's a service?

DAN YORK Mm-hmm. Oh.

ANNALIESE WILLIAMS So if you're joining us remotely, could you please go on mute? Thanks. So Maarten, you wanted to take this one? Thanks.

MAARTEN AERTSEN So this was a key discussion when the CRA came up. The question of, does this also include software as a service? The CRA does not, for the most part, cover software as a service. The NIS2 does for some types of services. So, I'm not sure where I anticipate things going, but at least that's with respect to scoping. I think there was another question later on, whether these regulatory obligations disincentivize the use of FOSS by ccTLDs. I don't know. I hope not, because I think it's a really big strength of our sector that there is a

great variety in implementations, which means that if you have a software bug, and software bugs exist, as an operator, you can choose a different implementation or rely on a second one. And currently, the DNS is open source, for the most part. So I guess there is still some awareness building to be needed with respect to some of these laws, because in a couple of years, there will be some solutions that can be CE marked and some solutions that cannot be CE marked, basically because of how these laws work. And if we see CE marking as a signal of quality, then I guess we need a little bit more insight into that it's all a little bit more nuanced than just having this label. So I hope not. I guess the future will tell. But that's my perspective.

DAN YORK I would add to that, this does vary widely based on the regulations that are out there. But you could see, though, where it might not, if you are forced to have a solid supply chain understanding and contracts around that. If you can't get a contract with an NLnet Foundation, but you can get a contract with someone else commercially, the risk management may bias toward that. And I agree with Maarten, that would not be a good way to go. But that is something that you are going to have to look at, and what is your own risk management, what's your own tolerance? What regulations do you fall under?

ANNALIESE WILLIAMS

Thanks, Dan. So the next one is, as software autonomy, sovereignty... Sorry, did we just... So I'm not sure how these questions are working. All right, so this one is CRA requirements on security by design, by default secure settings include the use of DNSSEC. Who wants to take that one?

MAARTEN AERTSEN

So, I guess this specific question would work for if you have a name server. You have a name server and it does online signing, or it does at least signing automatically. I could see how then you could explain the requirements of the CRA to require you to turn that setting on by default. But it's a little bit of a stretch. I think as a manufacturer, you have a responsibility to look at the essential requirements of the CRA and to meet them to the best of your ability. And then, before you make available this product on the market, check that you do meet these requirements. But I think we cannot simplify it to say you will always have DNSSEC on by default, because it depends on where the zone data is coming from. It's not that simple. So, I'll answer with maybe.

DIMITRIS ZACHARIAS

If I can add a second maybe here as well. It stems from the NIS2 Implementing Act. As I told you, there's a huge menu of stuff that entities can do, and one of them is best practices on the security of the DNS, which is another term for DNSSEC, but it's not something

that is completely prescribed upon. It's something that entities could use or could choose to use if they wanted to.

ANNALIESE WILLIAMS: I think we've done that one. But since we have got... There was one. I might just, if I may exercise discretion as the chair, there is a question in here that says, and I think it could be quite useful. So we do hear a lot about European regulation, but there is a question in here that says: Do you have any information or advice for non-EU ccTLDs in terms of whether the EU regulations apply to them? I just wondered whether, Elena, maybe is that one you wanted to take, or Dimitris, somebody? Yeah.

DIMITRIS ZACHARIAS: Thank you. My go-to answer would be no. I think jurisdiction- and territoriality-wise, what has maybe been a little bit more obscure from the NIS2 Directive refers to gTLDs rather than ccTLDs. I think the scope of the NIS2 Directive, specifically when it comes to EU law, only refers to the national administrations and structures of the 27 member states, so the ccTLDs of the 27 countries of the EU. Thank you.

ANNALIESE WILLIAMS: Thank you. And again, just a reminder, if you are joining remotely, could you please mute your microphones? Thanks.

ELENA PLEXIDA

Yeah. I'm going to add something. Maybe I'm completely misreading the question. Yes, agreed. But what caught my attention here is the ownership or governance of a ccTLD, and I pick on the words governance of a DNS operator. Just to say for the sake of the discussion, it's not about ccTLDs as such, but we can remind ourselves that in the context of the NIS2 negotiations, the decision was not to impose cybersecurity obligations on root server operators. And the idea there was that the governance, so that would be an intrusion to the multi-stakeholder governance. Same we had with CIRCIA in the US. They exempted again root server operators as well as other entities which are not necessarily defined, saying that whoever is under a multi-stakeholder governance should not be captured through legislation in the sense that they do it themselves. Just as something to put on the table. And since we're saying that, I will also mention that when CIRCIA was the trigger, and it was out in the cybersecurity obligations and what could be exempt from that or not. At the Contracted Party Summit, which was really close, the gTLDs had aired the idea, but that was just a discussion. Don't take it as anything further than that. Like, okay, maybe we should look amongst ourselves to do such cybersecurity requirements and reporting obligations in this space, perhaps as a way to tell policymakers that we're doing it. Again, might be relevant to the question. I just picked the other words, governance and the rest. Thank you, Annaliese.

ANNALIESE WILLIAMS

Thanks, Elena. And so I'll read this one out on the screen. So when it comes to security of ccTLDs, do you know if there have been any issues raised in the EU or elsewhere? Sorry, can we just go back to that? Oh, that was the one we just did? Yeah. Okay. Sorry. The next one is a test. Sorry. As you could probably tell, we haven't done this before in this committee, but it's good to try new things. I think this one's for you, Maarten. How do we get greater understanding of importance of FOSS given its criticality?

MAARTEN AERTSEN

I ask myself this question a lot, too. And so if you have ideas, I'm happy to hear them. My impression is that this has been shifting, and I tried to actually put this in my slides as well. Five years ago, there were barely any mentions of this concept of open source in, well, the area I'm most familiar with, EU law. And that is changing to the point where there's now headline pieces of a package labeled this way. That does not mean that in practice, when you run a registry, when you are a DNS operator, et cetera, that the people who make budget decisions have the same insight in the criticality of this stuff. And it follows logically from how this works, right? This is where the bits are handled, and it's not a very high-level topic. But I think as the economics of this space are so different, as there is regulatory pressure, it is very important that we make visible how all of this works. And I guess that starts with all of us to have that conversation within our respective organizations. Yeah. But I have no magic solutions. So sorry for the indirect answer, I guess.

ANNALIESE WILLIAMS

Thanks, Maarten. This is an interesting one. Is this affecting ccTLDs only or gTLDs as well? You've covered that one. So if we can just go to the next question. Dan, I think this one is for you. What layers of the tech stack can enable the greatest degree of autonomy, and how?

DAN YORK

I think the answer is that, sort of what Elena said, was that there's so many different layers at which we're having these conversations. Much of this is happening around the cloud layer, around the social media platforms. We're even seeing it around some of the connectivity layers, pieces around that in different forms. I think it partly goes to how do you define autonomy? What are you talking about? Is it for your nation, for your region, for your entity, for your organization? How do you look at what kind of control, what kind of choices do you have in there? One of the things we've had in this conversation around resilience, to kind of bring it back to the topic around this, is that everything is interconnected, going to all of the range of the suppliers, and if you're looking at DNS infrastructure, where is that running in terms of what kind of cloud systems, what kind of CDN systems. But we also increasingly have to look at the greater resilience picture, even looking at electrical power, and what kind of systems are there to ensure that that DNS infrastructure is operating. So I think you can answer this at kind of every layer of this. There's different answers

depending upon what your goal is, what kind of risks you're looking to reduce, what kind of autonomy you're looking to have in those layers, which is a really vague answer, because the answer's going to be different for every single one of you, I think, in some way. Maarten, did you have anything?

MAARTEN AERTSEN

Well, just to add a positive note is that at least in our space of Internet technology, some of the lower layers have been built in a way that enables distributed responsibilities to actually work in practice. So if you look at the routing system, it is really a collection of individual networks. If you look at how the DNS works, it is really a globally distributed database. That doesn't mean that in practice it is distributed, because there is concentration. But in this space, as opposed to some other spaces, there is the ability, from the ground up, to have that decentralization. And then I guess we get into the discussion of autonomy versus centralization, et cetera, and I will not go there now. But just to add one positive note to a complicated question. Thanks, Dan.

DAN YORK

Well, and I think you raised an excellent point, too, which is that the end goal is choice, is interoperability. When digital autonomy, when things like that, when those conversations lead to more choices and more interop and more places like that, they're a positive one. When those choices start to move toward where you're isolated, then we're starting to splinter and fragment in

ways that are not helpful. So that's really a key point, is why are you having this discussion? What is the end goal?

ELENA PLEXIDA

Which is exactly the reason why, as we were discussing before, it is great that this global conversation about digital sovereignty is not in our level. Our level is doing resilience because there is so much decentralization. That's what gives it resilience. Unfortunately, the digital sovereignty discussions tend to be about control, which would make the thing less safe.

DAN YORK

Yeah. Decentralization. All of us said if you go back to the earliest stages of the Internet, really, right, it was all decentralized and distributed. That was kind of the way everything was. We all operated our own email servers. We had our own web servers. Everything was that way. And then we've moved over time toward more and more concentration in forms, largely because it's been convenient, been easy, been able to scale at higher levels. But that does come with the challenges that are there. And yeah, we won't get into the whole... But the key point is how do we ensure we continue to have that level, the appropriate level of decentralization, and have it work in some way, keep doing what we're doing with all of this. And you're absolutely right. The DNS is a beautiful example because there are so many different kinds of different software implementations. There's interoperability. You can be using any of the different systems, and they all work well

together. That's the kind of thing we need to be looking at at every layer of the Internet in some form, rather than having it being in closed walled gardens in many of our layers.

ANNALIESE WILLIAMS

Next question. Thanks, Silke. We did that one. Okay, this is another complicated one, and I'm not sure who wants to handle this. But although the legislation you have presented has the objective of improving resilience, do you see a risk for actual Internet fragmentation coming from not complying with the many layers it requires? Is that one for you, Dimitris or Maarten?

MAARTEN AERTSEN

Yeah. So I'll specialize this question a little bit to give an answer. So when you look at the Cyber Resilience Act, the law with the goal of improving product safety about hardware and software, there was an early worry that entities based outside of Europe, for example, software makers, would stop supplying their software to Europe. And the early thinking amongst policymakers in the EU was, well, our market is very attractive. We have a lot of people living here, so surely people selling software will not abandon the EU market because that would be a bad business decision. What at the time they maybe hadn't considered as much is that a lot of this software in our Internet stack is actually free. And in that case, they were thinking about if we cannot meet some of these regulations, if they don't contribute to resilience of our software, perhaps the best outcome for us in a legal sense is to just not supply to Europe

because we can't actually carry the risks of not complying with this legislation. That was a bit of a doomsday scenario, maybe also a way to call attention to the issue, and I personally believe that this law has been tweaked quite a lot, and I don't see this currently happening with the CRA and with open source software. But that would have been an example of an objective of improving resilience and then maybe instead decreasing the choice available to, well, ccTLD registries such as yourself in the DNS space. So this didn't materialize, and I think that it's a big win for actually paying attention, talking to legislators, to make sure that doesn't happen. I could imagine this playing out at other layers. Perhaps the person asking the question had some in mind. I don't have the presence of mind to make up another one, so maybe something for the hallway later.

ELENA PLEXIDA

Yeah. Just to add to what Maarten was saying, and this is a very good point, also in the context of the NIS2 negotiations, there were discussions about operators possibly not providing their service anymore because these requirements did not make a lot of sense to them. So in effect, these different pieces of legislation would have the opposite effect, less resilience. But at the higher level, if you will, okay, one obligation here, one obligation there is not going to break the Internet. We're not going to see Internet fragmentation. Nevertheless, if we have more and more obligations that, if you will, intrude into the governance model that there is there, so little by little by little, pieces of what the multi-

stakeholder model does is supplanted, is replaced by legislation, national, regional, then yeah, little by little by little, all this model that secures the global Internet would be weakened and weakened and weakened. And that's not a good scenario. So yeah, one piece of legislation is not an issue. No way. But many that might be taking away pieces and pieces, it could.

ANNALIESE WILLIAMS: Thanks, Elena. I think we do need to wrap up this session, but thank you very much for your patience with our new testing of the Mentimeter question and answer. It was a new thing for us, so thanks for putting up with us as we were a bit bumpy. But I would like to remind you that this is a two-part session, so after the break, please do come back. We will be hearing some regional perspectives from colleagues. We have a European and an African region perspective. We have ccTLDs from Latvia and from Nigeria. But please join me in thanking our speakers. We have Maarten, Elena, Dan, and Dimitris. Thank you.

[END OF TRANSCRIPTION]