ICANN86 Seville | PF – Europe Space
Thursday, June 11, 2026 – 11:45 to 13:15 CEST

MAEVA DEVOTO: Hello and welcome to Europe Space. My name is Maeva Devoto and I'm the Participation Manager for this session. Please note that this session is being recorded and is governed by the ICANN Community Participant Code of Conduct, ICANN Expected Standards of Behavior, and ICANN Community Anti-Harassment Policy. Please observe the following guidelines to participate in this session.

Only questions posted in the Q&A pod would be read aloud during this session, as time permits and when directed by the chair of this session. If you wish to speak, please raise your hand in Zoom or otherwise as directed. When speaking, please state your name for the record and speak clearly at a moderate pace. I will now hand over the floor to Chris Mondini.

CHRIS MODINI: Hello. Hi, I'm Chris Mondini. I'm the Managing Director for Europe for ICANN and I work in the stakeholder engagement function. For the purposes of an ICANN meeting, it means I mostly stand up in front of audiences with a microphone and welcome you all. We're delighted to be hosting a meeting in the European region because it gives us an opportunity to gather a really diverse group of stakeholders to talk about topics of interest.

And I couldn't be more pleased to see that here in the room, we have representatives of our technical community partners. We have representatives from country codes, TLDs, we have gTLD representatives, we have other business stakeholder representatives, we have academics, we have some NextGen, we have some Fellows. And really, that's the point of really taking all of this multistakeholder expertise. And again, talking about issues of mutual interest and mutual concern in the European region.

And I think we might have one or two GAC or government people trickling in over the course of the session, which will also add a lot to the conversation. So, in addition to thanking all of you for being here, I want to thank the team and in particular Adam Peake and Elena Plexida, who have put the agenda together with all of your help and all of your inputs and all of the invited people who will intervene and share your perspectives.

I hope it's a robust dialogue and I hope everybody, whether it's your first ICANN meeting or your umpteenth ICANN meeting, will feel encouraged to share your opinion, ask a question, and advance to our group thinking on also some of these issues.

And also, please, I know it's the fourth day and maybe you're all worn out from meeting people and talking, but keep an eye out here in the room who's an expert on what and who's interested in what, and I'm sure you'll still make some valuable connections by the end of the session. So, with that ceremonial introduction, I'm

going to hand it over to Adam Peake to review the agenda. And thank you very much for attending. Thank you.

ADAM PEAKE

Thank you very much, Chris. Adam Peake. I work for Chris in the Global Stakeholder Engagement Team for Europe. First, perhaps an apology for the room. It's a little bit awkward for those of you at the back. It's an unusual shoeboxy kind of thing, isn't it? Please, as we go through the idea of the agenda, you can see the topics we have. So, we're going to go through legislative and regulatory updates, which, of course, Brussels produces a lot of this.

So, we want to talk about it and understand it from the various speakers, with the perspective of the various speakers. The ITU plenipotentiary is the geopolitical focus for many stakeholders at ICANN as we think about the activities outside of the specific ICANN arena. Of course, the WSIS+20, which we're at the implementation stage, and also looking forward to this year's Internet Governance Forum. And then some updates from the region.

And thank you particularly to Eoin from Irish government who will talk about the presidency of the European Council, which Ireland has, and Sandra Hoferichter, who's online to talk about the recent EuroDIG. Elena will run through the main thing. If we go to the next slide, you'll see this agenda with some of our identified speakers. What we want to do is try and run through this agenda quite smoothly and quickly, interventions for a couple of minutes, and

then to give all of you opportunities to comment, bring whatever discussion points you have on the various topics.

So, could we jump to the Google Doc? And I hope those of you at the back can see it. It's a little awkward. At some point after the meeting, I'll share it with everybody, but that's very difficult to do right now. A little bit as much as we can go. So, thank you, Chris. Thank you for the introduction. And we're at the legislative part. Yes, very difficult unless you have absolutely brilliant eyesight from further back than I am. So, Elena would you like to jump in.

ELENA PLEXIDA

Yeah, I should not turn off the mic. Thank you, Adam, for putting all this together, because it was really Adam that put all this together. I will just take a few minutes, not more, to start us off with mentioning a couple of initiatives that are currently going on, currently on the agenda. And of course, the EU obviously remains the most consequential jurisdiction for the DNS ecosystem.

By no means is this an exhaustive list of items that are there, nor the comments I'm going to just make briefly are exhaustive. We're very fortunate to have a lot of experts around the table, and I'm sure we're going to have a robust discussion. So again, in the spirit of just kicking us off, I'll mention a couple, a few. NIS2 has been there with us for quite some time.

We have a targeted amendment that now has come in with a Cybersecurity Act 2 vision. the end One interesting comment

observation on my side with the targeted amendment is that the NIS2 before as a directive, it was setting the minimum standards. So, countries, this is the lower you can do, then you can go further up.

The targeted amendment flips that around. It's like it's putting a ceiling. So, you can go up to here. Interesting to my mind that this is occurring and interesting to see how it plays out in our, in our space. The Cybersecurity Act, which I already mentioned, the revision, lots of things there. An interesting thing, just again in the spirit of kicking us off, to me is the supply chain obligations.

Of course, for the DNS ecosystem, there were already supply chain obligations, very specific through NIS2. The interesting bits for the Cybersecurity Act, if you will, is the way those are being put forth. So, the commission is going to have the power to designate, name suppliers and third countries as high risk. And that is left at the hands of the commission to designate any country they want in the future.

Now, of course, this is, and they have been quite frank about that, this is addressed to China, and China has already complained about that. But as I said, it is open. So, in the future, it could be any country at any event or in any supplier. So, interesting as a sense of DNS operators in the space. They use many different things from many different parts of the world.

What else? Digital Networks Act, obviously, an important one. Everyone was waiting for it, particularly because of the fair share

debate, whether it's going to be there or not. It's not exactly there. What we have there is the notion of, what was it, voluntary discussion with the regulator. And on my side, my comment is, this is very interesting, because is there really a voluntary discussion with the regulator? I don't know. So, if the regulator tells you, let's have a discussion, can you really say no?

Just an observation though. With respect to the fair share idea and how it is being treated there, we'll see. Another one from the Digital Networks Act is the, how is it? I don't remember exactly. Let me look at my notes. Optimized services framework that the DNA is introducing, is explicitly recognized that the primary technical method to deliver those optimized services is going to be network slicing.

There are some safeguards in the text so as not to cannibalize the internet from network slicing. The question I have at least is whether those safeguards are strong enough for that not to actually happen. It could be circumvented. Again, just offering some observations there. And I think I'll finish with the tech sovereignty package that was announced just last week. So, probably many people, including myself, haven't had the time to go through it in much detail.

My sense is it doubles down on the cybersecurity, sorry, the supply chain obligations as well. I will stop with just those, as I said, just to kick us off, because many people around the table are very

knowledgeable and have any observations to share with us and I will apologize for turning my back here.

ADAM PEAKE

Thank you, Elena. That's a nice introduction. Now, we have some speakers who have volunteered very kindly to jump in on a few topics. There's an order of speakers, but it doesn't have to be that order. We can go through them. But Hisham Ibrahim from RIPE NCC is the first, and we allocated you Sovereignty. Filip, who I believe is online, from CENTR. And thank you very much for joining.

Maaike Veenstra from the Government of Netherlands. Apologies for the TBC on your topic, which just means you have to cover absolutely everything. No, cover as you wish, and I think that we're grateful for that. And David Frautschy from the Internet Society who is also online and has some particular interests around IP Blocking and age restrictions. So, I don't know, Hisham, we have you first, if you don't mind if you'd like to make a response.

And the idea afterwards is to have all of you please jump in with your comments and observations. We've allocated probably another 20 minutes for this and we'll try and run through the agenda. Thank you. Hisham, over to you.

HISHAM IBRAHIM

Yeah, sure. Thank you for that and good morning, everyone. I'll try to make a short intervention and then as the discussion evolves maybe I'll add a little bit more into it. On the topic of sovereignty

in general, we're seeing that word coming up a lot in many of the discussions.

The interesting thing is it's used differently in different contexts, and while people sitting around the table might think they're talking about the same thing, it's very important that we clarify because in some contexts, sovereignty is seen as control, for example, or more need for control, which generates this like knee-jerk reaction from a lot of people that do not want to see that.

In other cases, it's about building capacity. That capacity could be either public infrastructure. It could be done through investing more in building infrastructure, whether private or public. It could be done within the region, or they could be looking into partnerships. So, it very much differs per region and how they look into this.

The internet will always have dependencies. There is no one network, there is no one country that can claim it has all the content and all the direct connections to all the end users around the world. And I highly doubt we will ever live to see something like this, even if anybody has plans to do that. So, there will always be a point where you need to hand over packets or data or something to another party where then you need to have meaningful trust and understanding of how this needs to be handled.

And I do think the sovereignty discussion is something that I believe governments are raising very legitimate questions about, well,

control, resilience, but mostly about choice. And I do think that's the key thing here where we need to be focusing on.

If these discussions around sovereignty provide more choice, more options, more meaningful choice for people, that is definitely a good thing. That is something that you would want to see, again, as a recovering techie and somebody that reads a lot about policy these days. More diversity, more options is a good thing for everybody and nobody would ever complain about that.

It's when it starts crossing that line into mandating, you should only be using this, or you should be only hosting there, that is where you can begin to find some overreach there. So, basically, what the litmus test here is, is by pursuing these discussions, are we providing more meaningful choice that still allows for the global interoperability to happen? Or are we then compromising that in the name of control? I'll leave it at here, and I'm happy to jump in with the discussion later.

ELENA PLEXIDA Thank you, Hisham. And please, anyone that has comments on this topic, and I'm sure we can discuss just this topic forever, jump in. I will suffice it to say that, first of all, I couldn't agree more with the comment you made, that it is a very legitimate discussion, absolutely, to have this discussion. At the same time, this discussion, it doesn't matter what the definition is, is not really about us.

It's AI, cloud, chips. And I want to say this is a very good thing that the digital sovereignty discussion is not about us. We should not make it about us. This community, as the RIPE community, as all the technical organizations, have always been all about resilience. So, we keep talking about our resilience and how we do it, and we're there. Of course, things can be better, but key message, let's not do anything to make it about us as well. And I see Pierre already.

PIERRE BONIS

Thank you very much; first of all, to elaborate on that sovereignty topic. As you said, Elena, whether it's in the Cyber Act or on the new European package on European sovereignty, digital sovereignty, this is a hot topic. I just wanted to add two things. The first thing is that the chips, the dependencies that are on the hardware, they are our problem, I guess, because most of the ccTLDs, for instance, they need to buy these products.

So, it's not only the DNS rules, it's the way that we make sure that the supply chain is still available for us. So, I'm not very sure that a European directive will solve the problem, but I think it's very important to keep in mind that these technological dependencies on hardware and sometimes software or licenses affect us as operators. That's the first thing.

And the second thing maybe is that I think it's always important to raise transparency about the dependencies. And that may be the good thing about this sovereignty discussion is that, as you said, no

one is going to govern Internet on its own. But if you look, for instance, the market share of Cloudflare in terms of DNS resolution, I don't know if it's a good or bad thing, but it's concentrating a lot of traffic, for instance, and this is important to have transparency on that. Thank you.

ELENA PLEXIDA Thank you, Pierre. Yes, that's a very interesting thing always to keep in mind. That's why I kind of, at the first five minutes, I talked a lot about the supply chain thing, because of course all these things are going to affect the DNS operations and the operators as such. The other bit of it is what I was trying to say, I guess, is like, take the EuroStack report, which kind of was the first document there that kicked off the discussion.

And he was putting down what are the items that we policymakers should be looking into, the tips, which of course, [00:17:32 – inaudible] yes, are going to affect us. And there was one paragraph there, one very small paragraph that was saying, yes, we talk about cloud. Yes, we talk about IAI. But down the future, maybe we want to look at the DNS as well as a topic to be included in the global debate, that is something. Anyone else, please?

ADAM PEAKE We have a hand mic if anybody further back would like anything. Wave and you will get the microphone. But I'm not speaking into

the microphone, so. Anybody at the back, any comments around this topic, or we can move along. I feel like an auctioneer.

HISHAM IBRAHIM

I can maybe just add something very quickly here. Indeed, it's that word that's been said a lot here, two words actually, which mean pretty much the same thing. The supply chain, that's absolutely what it's being looked at. If you look at the package that was released on the 3rd, it does have indeed the chips, the AI, the Cloud Act, and it looks into those interdependencies.

And I do think that it's smart that you look into where your interdependencies are because they always exist. You mentioned concentration of content. I do think it's also important, and I think this is a point Elena's making, is understanding what layer are we talking here? Are we talking content?

Are we talking technical operations? Are we talking where do we need to be addressing this? To do a shameful plug-in, I do have an article on this if anybody's interested on it. It's on RIPE Labs that details this in a little bit more, but to allow the discussion to go, I'm gonna leave it at that. Thank you.

ELENA PLEXIDA

Thank you, Hisham, for the shameless plug-in. Next up we have Filip.

ADAM PEAKE And Filip, you're online, I believe?

FILIP LUKAS That is correct. Hello everyone and thank you very much for having me. I'm Filip from CENTR, which is the Council of European National Top-Level Domain Registries. And I'll say a bit about the Cybersecurity Act and the financial regulation that we see in the EU. As I already mentioned, among other things, the Cybersecurity Act 2 includes provisions on the trusted ICT supply chain framework, which basically will apply to all essential and important entities under the NIS2 directive, which the idea there is to assess the cybersecurity and non-technical risks associated with suppliers from outside of the EU.

The risk assessment can be either started by the European Commission or by a group of EU member states, and the assessment would include the assessment of ICT assets, supply chains, main threat actors, risks and vulnerabilities affecting these assets. Well, if the risk assessment actually shows that there is indeed a risk for a certain supply chain or key ICT asset, then for the provision of the essential and important entities such as ccTLDs, the European Commission then may prohibit through an implementing act using, installing, or integrating these ICT components from hybrid suppliers.

The Commission can also subject the essential entities to additional auditing or for example require diversification of their ICT component supply. There's also the assessment of countries

and that whether a specific third country presents a structural risk to the supply chains. Then the assessment looks at a number of things. For example, whether the third country laws require entities under their jurisdiction to report vulnerabilities.

Another metric is whether there's effective judicial remedies or whether actually there are threat actors that are located or controlled by the country or located in the country. And then again, if that is the case or if that is the result of the assessment, the Commission might then, through an Implementing Act, prohibit essential or important entities from using or installing these components from entities established in these countries.

And in addition, the high-risk suppliers that would be determined through the implementing acts by the European Commission would also be precluded from participating in European standardization activities, applying for EU certification or participating in public procurement. Now, in CENTR, we are currently in the very final stages of voting on our position, which the vote is actually ending tomorrow. But I will share a bit from our own perspective already.

So, we focused on five main points, which that the risk assessment should be evidence-based and that the prohibition of any high-risk suppliers must actually be based on tangible and evidence-based security risk, and there must be a clear framework that considers the nature of critical infrastructure and the specific equipment that the essential entities use in their operations.

The second point is that the impact assessment before the decision becomes binding must be developed in consultation with the affected entities before any exclusion of key suppliers is actually binding. The third point is on the phase-out. So, if there is a phase-out of affected ICT components or supply chains, then the phase-out must be reasonably long, I believe we said 36 months by the minimum, depending also on the specific item.

And if applicable, there should be possibility to apply or to request meaningful compensation for having to replace the supply chains, especially in the absence of viable alternatives or when in-house development is actually needed to replace the high-risk vendor. Furthermore, there's the issue of direct contractual relationship because the proposal, the Cybersecurity Act 2 proposal actually recognizes DNS as a key ICT asset for the functioning of electronic communication networks, which should or might result in the sort of assessment of the ICT supply chains of the DNS.

So, what we would highlight is that the ICT supply chain definition needs to be revised to limit the scope only to suppliers with direct contractual relationship with the affected essential entity, so that the definition avoids general statements regarding key internet infrastructure protocols such as the DNS. And finally, the proposal also expands the ENISA mandate that's actually one of the three main pillars of the proposal.

And the ENISA should also support high-criticality sectors under the NIS2 directive, such as ccTLDs, by providing them with best

practices and guidance on available tools and procedures. So, we just highlighted the fact that the expanding of the mandate is reasonable. However, the ccTLDs would like to highlight their autonomy in setting the policies and their governance independently.

That would be my bit for the CSA. I do have a very short intervention on the financial regulation, which unfortunately is a thing that is staying with us. And that is specifically the proliferation of DNS-level enforcement across financial legislation. The initial source of this is actually the Consumer Protection Cooperation Regulation, which a few years ago introduced a language or an article that allows competent authorities to order domain registries or registrars to delete a fully qualified domain name in order to prevent consumer harm.

So, that is part of the Consumer Protection Act. However, the same language was then adopted in the markets and crypto assets regulation, almost identical language. And then it was also included in the proposal of the financial data access, which is currently being negotiated. And also in the very recent payment service regulation, which is in the final stages of the negotiation, where it was added in the trial negotiations by the Council of the EU.

So, in the deprivation, although it was not, at least from my recollection, it was not in any of the in the MICA, the Markets and Crypto Asset Regulation, it was not actually enforced yet, but

indeed it creates this enforcement power that can be used on registries to delete the fully qualified domain name.

And finally, an interesting point is that the payment services regulation in the final document that I had the chance to see, there's also in the recitals, so not in the articles themselves, but in the recitals, there is a reference to the need for the payment service providers to use tools that prevent fraudulent replication and misuse of the payment service provider's domain name which is a part of the anti-fraud provision and hints at potential additional tools that the provider should use, I suppose in this case would be DNSSEC. But we'll see how the final document looks. It should be finalized any day now and then we will know for sure.

ELENA PLEXIDA

Filip, thank you so much. This was really, really helpful and deep in expertise. I just want to extract and highlight some things that Filip already told us that merit particular attention. So, Filip talked to us about the financial regulation. He said there was language about domain names or DNS that was in the consumer stuff and then that also got into the financial regulation and also got into the crypto regulation. This also is a very important word that we need to be mindful of.

In Europe, there's a lot of copy-pasting of DNS related language to also go to other things. That's a trend to be definitely mindful of. And the other thing that Filip told us, which is in relation to the CSA, and that goes back to what exactly Pierre was saying before, there

are obligations, DNS is included as a component of core network infrastructures, key ICT asset, and that goes back to what Pierre was saying about all the operators being there because of their operations. Very important. And the ENISA mandate, finally.

There was language about the ENISA mandate and the public core of the internet, including the DNS and other things, already in the CSA the way it was. It's still there, somehow augmented. It's giving a role to ENISA, which is fine as long as it is recognized that there is the autonomy of the ccTLDs, that there is the multistakeholder model and what it is that they're doing, we're doing, and all the organizations are doing, so.

Yeah, fine as long as this other space is not forgotten and we move to ENISA coordinating exactly what if the coordination is happening here. Any comments? Hisham, yes.

HISHAM IBRAHIM

Maybe just very quickly, and maybe this will bridge also to your next topic on this too, but as part of the NIS2 simplification process, one of the things that we put forward as RIPE NCC is, indeed, we just said similar to what you said, we encourage the Commission and ENISA to consistently apply a strong multi-stakeholder approach and work with the relevant actors in accordance to their representative roles and responsibilities.

We're addressing the core technical functions of the internet, especially in relation to the CSA 2 proposal draft as well. So, what

you said about making sure that language in different acts are actually consistent and that we're looking across all of them, not just having tunnel vision on one, is important. Thank you.

ELENA PLEXIDA: If I got that right, this is a comment you sent into the public consultation, or? Yes, go ahead.

ROMAIN BOSC: Hello. I might comment on that because I was also involved in drafting the inputs from the RIPE NCC. I'm Romain Bosc, Policy Officer of the RIPE NCC. Indeed, in the context of the consultation on the CSA 2 and the NIS2 simplification, we had three main comments.

The first one is more of a positive tone because we welcome also the simplification effort that the Commission is now also pushing forward, namely the creation of a new regime for or size cap for DNS service provider, for small and micro-DNS service providers, and a new regime for mid-caps enterprises.

So, that is to be welcome. I was reading this morning, there is a new OECD report that is looking at the whole cybersecurity legislation landscape in the EU and there is this interesting data point that basically the cost of compliance across the EU is estimated at 30 billion annually, 30 billion euros.

So, I think there is a need maybe to support also a bit more simplification on the compliance side. The second main comment

we made relates to the obligation for entities to register IP addresses to their authorities. And saying that the main purpose of this is to improve policymaking, the simple fact that there is no impact assessments or cost benefit analysis on this measure, and we hear also from even the regulatory authorities themselves that they are facing issues in also collecting those so-called IP ranges.

So, with the aim of improving visibility and compliance for the entities, but also improving the life of the supervisory authorities as well, maybe explaining what is the intended purpose of this. There might be some security benefits, but what are the techniques that they are going to use? How intrusive and effective those techniques might be is a key question.

So, again, having this conversation with the authorities is key. And the third main point was about precisely the role of ENISA and maintaining a very strong multi-stakeholder approach and ensuring close collaboration between ENISA and the technical community. So, that was it.

ELENA PLEXIDA Thanks, Romain. Sounds to me there is also an element of duplication with what you said there, like the national authorities will maintain a list of the IP allocated. But you have that list anyway as well. Just saying.

ROMAIN BOSC

Maybe also adding to the point about duplication, looking at the next item on the Digital Network Act, there is one particular aspect that is of interest. BEREC is being tasked to work on a so-called EU Resilience Properness Plan. And interestingly, yesterday, BEREC put out a paper, a position on that.

It's precisely calling for caution about the risk, again, of duplicating supply chain risk management measures, network security measures, and duplicating what is already there in the CSA, in the NIS2. So, now through the DNA, there is again another layer of complexity and duplication that also is on the table.

ELENA PLEXIDA

I also want to make a shameless plug here. The ccNSO held a very interesting session on resiliency overall across the board. Of course, EU matters were touched a lot upon because still is the most consequential jurisdiction, but it was a very good session I found from the ccTLD looking at the resiliency part and how it affects the ccTLD, of course, operators, but broadly the ecosystem, my shameless plug. Pierre.

PIERRE BONIS

Yeah, thank you, Elena. Very quickly on the IP requirement, as you said, it can be duplicating with what RIPE does. I'm not very sure we're talking about the same thing. And the National Security Authority asked us to give them the range of IP we are using for

servers that are serving essential services from essential entities, which I guess doesn't have this information.

And by the way, they don't need it. So, it's not really duplicating. Since I totally agree with why do you need that for and what are you going to do with it? So, I totally agree with the RIPPE position, but it's not duplicating right mandate, to be clear.

ELENA PLEXIDA Thank you for qualifying that, Pierre. I must admit I didn't go that deep on the numbers side of things. Thank you, Pierre. And then we move forward to Maaike.

MAAIKE VEENSTRA Hi, everyone. My name is Maaike Veenstra, and I am working for the Dutch government, the Ministry of Economic Affairs and Climate for the Department of Digital Economy, and I'm also the Dutch GAC alternate in the GAC. One of the topics that I'm working on is Internet Governance, of course, but the other one is EU coordination.

So, I'm very happy to be invited to this session. I'm not involved generally on expert level because this EU coordination is quite big, as we all know, but generally more like guarding the topics of our department and looking for a consistent input throughout the Telecom Council and the Telecom Working Groups. For this group, I actually thought it might be useful to talk a bit about our national implementation of NIS2, and specifically the Article 28.

As we all know, Article 28 leaves a lot of room for national interpretation, and this can be both a blessing and a curse, because the DNS infrastructure is, of course, in essence, a cross-border infrastructure. But despite this being a challenge, as policymakers, we try to see the bright side and use the liberty of national implementation provided by the NIS2 also to our benefit.

So, we met with policy experts on NIS2, our regulators, our registries and registrars to discuss how we would be able to implement this Article 28 in a way that will work for all of us, like truly in the spirit of the multi-stakeholder model. We compared the ICANN rules to the NIS2, to the rules of the regulators and registries, to see where they overlapped, but also where they did not. And we tried to develop a common framework, so to say, for the implementation of Article 28.

The ultimate goal was, of course, to show an industry best practice, because the implementation of specifically Article 28 can be quite challenging for many member states. And we tried to show that as the Netherlands, we could show this perspective and also a true bottom-up process and not top-down.

So, the current status of the national implementation of the NIS2 is that in April 26, it got accepted or it got through the parliament of the Netherlands, and it's now scheduled for agreement in the Senate in early July. Hopefully we will implement the directive somewhere mid-2026. Following that, we also have a testing phase of about 18 months to see what works, where we need to improve,

where we need little tweaks and changes. And we will see the outcome of that.

So, we don't know yet. But if you're interested to know a bit more about this and how we did it and this process, of course, feel free to ask either me or my colleague from the Netherlands, and we will be happy to clarify and answer your questions. Thank you.

ELENA PLEXIDA Maaike, thank you so much for being here with us. It's really appreciated. Anyone has any comments? Of course, Hisham has comments.

HISHAM IBRAHIM Of course, Hisham has comments. No, I just wanted to, as an organization based in the Netherlands, we were very happy with the approach the government took there, whether it's the ministry or the RDI or others, in doing exactly what Michael was just saying, understanding what any step would mean for implications for broader Internet governance, what this means, and showing a lot of understanding and dialogue. So, that was very much appreciated. I just wanted to attest to that. Thank you.

ADAM PEAKE I think that goes to the government of Netherlands and others who are also doing consultations about the new round and other activities there. The GAC is, like all of us, learning how to engage with these processes and it's very good that you're reaching out

across governments and also the stakeholders. Pierre, I suspect Article 28 was mentioned and it's one of your favorites.

PIERRE BONIS I love it.

ADAM PEAKE Thank you.

PIERRE BONIS And very quickly, first of all, we all have to commend the approach of the NL government. Still, there are some news, I don't know if you saw, that the European Commission is aiming to sue at least France and Spain and maybe other countries for not having transposed yet, which is something in the multistakeholder model, I would like to draw the attention of the government on something.

I mean, when you validate a directive that is so vague and complex that you are not even able to transpose it in the timeframe that you said was compulsory, expect those who will have to implement it to have hard days. And I think this is a lesson that we all have to learn. I mean, this is so vague that even the governments cannot transpose it. And then after they say this is compulsory and if you don't do that, you go to jail.

So, there is a problem with that. That's the first point. And the second point, and I recognize this is very important, that because it's a directive and it has to be transposed, the various situations of

various countries would be recognized as long, of course, as it is coherent with the directive. And I hear, and I will end with that, I fully understand that some countries will transpose this Article 28 with an approach of, let's say, 100% verification and maybe ex-ante verification.

I would say, I mean, do whatever you want. This is your problem. But this is not what is written in the directive. And in the directive, this is said that you have to put in place procedures that aim to guarantee the quality of the baits, which doesn't mean 100%, which doesn't mean ex-ante. And in some context, and that's not because some countries don't want to do that anyway.

I'll give you a very concrete example. In some countries, and in France particularly, the EID scheme is not very well advanced. So, in some countries, this is pretty easy to say, okay, use the EID that you use. 10 times a day to register. In some other countries, maybe it will be very easy and possible in two or four or three years, but for now, you have to ask for photocopies of ID cards, which is not at all the same and you don't make automation on that.

So, I really hope that the best practices that could arise from these exercises in you in different countries will be seen, recognized, but will not be seen as the example to follow in other countries. Otherwise, we're going to have some implementation problems. Thank you.

ELENA PLEXIDA

Absolutely. And as Pierre said, the directive doesn't say anything. It says best practices. Just to qualify Article 28, we have the whole NIS2 cybersecurity related things, and then we have one particular article that is very specific to the DNS and specifically to registration data. And this community has talked extensively about this article.

Also, just to add up to what Pierre was saying, yes, it's difficult to implement it, of course. And now you already have an amendment on the table on an NIS2. Anyone has any other comments on an NIS2? Okay. Then we go on to David, who's with us online.

DAVID FRAUTSCHY

Hello, Elena. Hello, Adam. Thank you for inviting me. I'm David from Internet Society based in Brussels, and I'm going to speak briefly very briefly because I know we are not very well on time on IP blocking on age restrictions. So, IP blocking for those who you don't know it's about protecting copyrighted content through breaking the internet.

But at least setting up some IP blockings, the problem here is that of course you cannot block just one website that is doing wrong, that is doing illegal content by blocking IP addresses. It's not like a telephone line that corresponds one to one to a home or to a user. IP addresses most times are shared, so it happens that if somebody issues a blocking order, this will have the consequence of blocking

many other services that are legitimate and doing their businesses, you know, with they should not be blocked.

So, there are strong concerns in Spain. You are right now in Spain and I don't know if you are aware, but in Spain, soccer, football, soccer is a big game. Today, the World Cup starts, so you will see that at some point this afternoon, this evening, the city will stop completely. Everybody watches the soccer games. But what happens is that it's very expensive, so people find alternatives that are not legal.

So, the right holders of soccer games in Spain, La Liga, is an organization that organizes the championship has a judge that IP blocking is the right way forward. And the judge, well, probably the judge, he doesn't understand how the internet works and he issued a ruling that allows for these IP blockings. Now, it is important to understand that even notorious websites have been blocked in the last months during weekends when soccer games take place. Not only the City Hall of Madrid website, but other notorious websites.

And these days when websites are not just contained in the sense, because sometimes content on the websites come from other websites or even payment systems are done in other websites. So, when you do your e-commerce thing and you fill in your purchase and your public data, this data jumps to another website that verifies the payment and then comes back to the vendor and says everything is okay.

Well, one of those companies that does the verification was blocked on one of these blockings one weekend. So, it is a mess. There are voices racing, but the evidence is not coming to the judge. So, it's a bit of a nightmare. At the ministry level, at the regulator level, they do understand what are the consequences, but they say okay this is a judge that has ruled that this can be done.

So, there are interesting developments. The congress in Spain just passed a non-binding, how do you say it? I don't know the expression. It was voted by all parties except right-wing asking for language on proportionality when this DSA is transposed into Spanish law. So, this is in the right direction, but it takes time. Now in France, they are debating a new law on sports. It includes many topics related to the management of sports clubs and so on. But there is this new Article 10 that allows for the same thing, IP blocking.

And I want to raise the call for action to the community. It's now time to send amendments to the French government so that this is changed, proportionality language is needed, avoidance of collateral damage is needed, and perhaps it's important also to include a liability issue here for those who request IP blocking. So, there is no incentive for these people to minimize IP block requests.

They don't have to pay anything. If third parties are affected, they don't have to pay for the consequences of revenue, lost revenue, and they don't have to pay even for the implementation of the blocking. So, we know, of course, that executing the blocks,

executing the blockings is time-consuming, resource-consuming, but these people that issue the blockings don't have to contribute.

So, perhaps, this would be interesting to increase, to create an incentive not to just shoot with a canyon instead of doing something retargeted. Now, the other thing that I wanted to talk about is age restrictions. Just everywhere, countries around the world are discussing how to do this. And we have identified many, many concerns. It's mostly privacy concerns. These solutions, in most cases, they capture too much data.

Normally, they store it in databases that are, of course, honeypots for hackers. I see a couple things, and right now, you want to interrupt me now or at the end? if it's IP blockings or H restrictions, let's take it as this type of blocking. Andrew. Okay I'll continue with the H restrictions.

ANDREW CAMPLING Sorry, I can wait to finish. It's about blocking, but yeah.

DAVID FRAUTSCHY No, go ahead with the blocking. Yes, please. No.

ANDREW CAMPLING Andrew Campling for the record. To clarify first, I'm not a fan of the legislation in Spain or Italy. I think it's badly done. But two buts. One is what would we expect if we increasingly take steps to

obfuscate some of the other potential methods, such as DNS blocking, by doing encryption on the DNS and so on.

So, essentially, it's not surprising that you leave legislators with one thing, which is IP blocking. And then the fact there's collateral damage, again, well, that's a design choice of CDNs, you don't have to co-locate and share the addresses. So, if you like, that's on the industry and the design choices that it's made. You can't then say, but collateral damage, therefore we shouldn't do it.

Implement it differently, give different choices, and then you wouldn't have that issue. And then just second quick point, it's not just about copyright protection. Again, if you want to have business disruption measures for things like, dare I say, commercialized CSAM sites, again, you increasingly don't have many options other than IP blocking. So, we've caused the problem by ruling out the other tools. You can't blame the regulators for using the one tool left in the toolkit. And if that has consequences, well, that's on us. We should be smarter. Sorry.

DAVID FRAUTSCHY Okay. Thank you, Andrew. I sent on the chat two documents that we published recently. One of them is on IP blockings and the other one is on DNS and we explained there why these are not the topic tools. So, on the age verification, age restrictions, we are concerned about this proposal by the European Commission to create a blueprint. This is a set of recommendations on how to set

up an app to verify age. So, in principle, it looks fine because it's only a token that is stored on the device of the user.

This token would just inform a yes or no to a request of if the user is under or above a threshold of age. So, imagine some 16-ager trying to access social media and there's a social restriction for under 16. So, this token would say, okay, this individual is above the age. It's only a yes or no. Or imagine a site or a website that is intended only to be used by minors. You don't want adults there because you want to avoid harassment or other kinds of illegal activity.

So, you want minors only, so you ask if this individual is, yes or no, under 18 and the token will do this. Only that information, no name and no other data. So, this looks fine, but then how you fit these tokens. If you need to fit this token by showing your ID to the camera of the device, this can be a privacy. This can probably be a privacy, capture too match data.

There's another option there that you would go to the post office and over the counter show your ID and the official there would fit in the token. But then what happens with countries that don't have post offices anymore, thinking about Netherlands or Denmark. And then there are some features there that are optional to be implemented or not, or member states do not even need to follow the blueprint. They can do their own.

So, what we see here is a situation where either country will set up a different version that will not be usable for people who travels,

and at the end, we see the commission using the wallet to do this thing of age verification. So, this can be very tricky because there's a lot of information there. So, we find it legitimate that countries set up a system to avoid that minor success content that is not appropriate for them.

Think about phone, think about gambling, but of course, there's a responsibility to be taken by social media whether to tag the content for whether this content is appropriate or not, do some moderation. But we think it is important to find a solution that is very preserving. And well, at the Internet Society, we're going to develop some recommendations on this. And yeah, I'll leave it there. I know we are with time constraints. So, happy to take more questions.

ELENA PLEXIDA Thank you so much, David. And indeed, I mean, to pick up on Andrew's comments, and I think you're absolutely right, policymakers are looking increasingly into this space, and why not? And courts as well, and why not? And this is perfectly fine. I guess it's just a matter of the trend is there, we see it, courts getting more and more involved.

I guess for this community, it means it creates a space or, if you will, a need for enhancing the understanding. Perfectly fine to do that. Just understand what is the technical reality. So, what can you achieve through what? If I can put it that way. Hisham?

HISHAM IBRAHIM

Could I just comment on the IP blocking bit? Because, again, IP addresses. It's very important, and I mentioned this before, to understand what layer are we really talking about here and where to address the real issue. If it's a content-related issue or if it's a technical operations of packets moving back and forth. And trying to find answers in the wrong layer could have bigger ramifications and amplifications.

And that's where, as you're saying, that needs to be better understood, right? To Pierre's earlier point about registration of IPs and stuff, because we did have indeed the intellectual property people and the leagues coming to us as RIPE NCC and asking for more information about who is exactly using what, which is information we do not have, we give out big blocks to operators and we explain that to them.

But more and more we're seeing, because there is indeed a lot of money at stake here, these groups are trying to position themselves to have similar treatment as LEAs and law enforcement requests and such. Having them have better understanding of what can and cannot be done and what should and should not be done in every layer is a continuous dialogue.

We've had that years before. They've looked into other spaces. They're coming back to our space again. So, it will be a continuous effort to make sure that these issues, again, which are real, are

addressed at the right level, which is, again, hosting and others rather than DNS and IP.

ELENA PLEXIDA Yep, agreed. And finally, to the other part that David was informing us about, of course, it's about age verification has to do with social media, obviously. But going back to what again, Pierre was saying earlier, as verification things progress around and best practices in this area progress, that is something that would then concern eventually this community. So, yeah, it is there. It's not entirely relevant to us. Right now, it might be, but in the future, not so. Yes, please.

HUGO RAMIREZ Hello. Hugo. Well, I live in the UK, we've seen age blocking in some sites, and well, first of all, youngsters are using VPNs, and so, it's not being useful at all. But the question, if we do this with age, we can start to get more data besides age and with social media and we're profiling people, and with AI models, we can start training models.

And I suppose this information starts to live with the ISPs. So, I don't know if these are subject to regulation as well, because capturing information about people. I mean, this was more of a question rather than…

ELENA PLEXIDA

I'm not sure if the question was about safeguards that are in regulation. I have to tell you very bluntly that because it is beyond the ICANN remit as such, we are not paying attention to it at that layer. It had to do with the layer levels that we were discussing before. But if anyone else in the room is paying attention to that. My apologies. Okay. So, we spent a lot of time on the legislative or non-legislative initiatives front, but truth be said, as -- okay, Fredrik, please.

FREDRIK LINDEBERG

Sorry, I just want to make one comment here, which goes through all of the tracks. Fredrik from Netnod here, root server operator, secondary DNS operator, ISP operator, and distributor of national time and frequency. So, what's happening here is that we have different frameworks, which affects how we do things, right? It doesn't matter if it's IP blocking, age verification, how we run DNS, et cetera.

I think it's very important that we take a step back and think about if we in Europe, or the EU for that matter, are doing things at a technical level differently than others. So far, the legislation is targeting processes, right? We have different risk mitigation processes, risk reporting processes, incident reporting processes, and we should all start to be aware of when legislation makes us do technical things differently.

Because we cannot run DNS differently in Europe compared to the rest of the world. The UK cannot run DNS differently. Everybody

has to run DNS the same way. Everybody has to do IP addressing and routing the same way, et cetera.

ELENA PLEXIDA

Excellent point. Bringing us all back to the core of why we spend so much time discussing these issues. And with that, we go to the WSIS+20 implementation a bit. Oh, sorry. Number three, sorry. Over to Janis.

JANIS KARKLINS

Yeah, thank you very much. Janis Karklins, for the record, head of government engagement. So, 2026 is the year of ITU plenipotentiary conference which is happening once every four years. As far as it stands today, it should happen in November in Doha, Qatar. And apart from electing all the senior officers, Secretary General, Deputy Secretary General, three directors of bureaus, adopting budget, conference also will be negotiating a number of resolutions.

Some of them are linked with internet, internet governance, questions, IP addresses, IDNs and so on. So, we're looking into preparatory process. Of course, we at ICANN, we're following very closely that process, attending all the regional preparatory meetings where we are welcomed and allowed to attend. Two regions do not want us to be following their preparations. Nevertheless, we're following through proxies.

Since we don't have time, what are the major risks that we see at the plenipotentiary? So, first of all, that is a potential push to more intergovernmental impact to internet governance. So, the manifestation of that is ITU Council Working Group on Internet is government only, and we are trying to persuade governments to open it to all stakeholders.

It would be in line with the decisions of the WSIS+20 review conference. And broader speaking, we will attempt to or encourage member states to use WSIS+20 language on multi-stakeholder approach to internet governance, also in ITU resolutions.

So, that is the one kind of risk. The second one is the risk of decision to convene in probably 2028 the new World Conference on International Telecommunications. The last one, which took place in 2012, failed to agree on a new set of telecommunication regulations. As a result, for the moment, there are two regulations. And clearly, there is a pressure to include in international telecommunication regulations also internet-related issues, and that is a serious risk.

Maybe I will stop here. There are, of course, many other things that we will be following. IPv6 discussion, that ITU should or shouldn't become a RAR, or whether they should be involved in promotion of IDNs and Universal Acceptance. I'll stop here on Plenipotentiary.

ELENA PLEXIDA Tatiana, you have a comment?

TATIANA TROPINA Yeah, so maybe going a bit into details, what we are following here. So, Janis already provided outlines of the major concerns, and I have to say that ISOC we have very deep into the preparation for the ITU plenipotentiary since last year already because some of the regions started their substantive meetings already. in November, December last year. We are attending the same as ICANN.

In two regions, we are not welcome, RCC and Arab region, but we are monitoring through proxies and friendly connections. And just for anyone who is wondering like we are in Europe here and why we're talking about this, I must say that Europe probably is the least problematic region for us in terms of reparation, more homogenous, more friendly to multistakeholder and internet governance.

But ultimately, the European regional position will be affected by other regions and the final negotiations will be the trading and negotiations between these regional original proposals. So, from what we see now in relation to concerns Janis raised and to what we are monitoring, the regional discussions are still developing, although some regions are quite closed or already approved the proposals related to internet-related resolutions.

And briefly, what we are monitoring at the Internet Society, of course, kind of maybe less relevant to this group, we are looking at

connectivity and infrastructure. Because, not surprisingly, after some countries like Saudi Arabia, for example, dissociated themselves from community-centered connectivity solutions, community networks, at the WSIS+20 final meeting where the outcome was adopted, we are very much worried that the connectivity will be linked to the governments only and community connectivity solutions would be excluded.

We are following also some thorny topics like, for example, LEO Satellites Regulations, which are on the agenda for some regions. Digital inclusion is relevant and consistent threat for all of us. And it's not only about the IDNs, but also about addressing the need of developing countries and having some more flexible approaches to building connectivity again. And now coming to the most relevant issues, these are the internet-related resolutions. Janis already mentioned them.

So, internet public policy issues, group on internet governance, whether to make it closed or open to stakeholders, multilingualism, IPv6, WSIS follow up. And we are closely watching for the language, especially in regional proposals in some regions that will shift the power from the multistakeholder model, from inclusive models to more intervention from the governments, for example, in the IPv6 deployment, in the role of the RIRs, in the standards making, so rather through existing models and technical community to others.

We are also countering in this regard the proposals that will try to insert very vague language related to AI and quantum into internet-related proposals, because this again opens more doors for the governments and the ITU to expand their mandate. Of course, the WICIT, World Conference on International Telecommunications, which can potentially review the international telecommunications regulations and expand the ITU mandate and include more governmental role, is very much on our radar.

As Janis said, 2028 might be the year. And our mandate is broader than ICANN's, and we know it, so we are following and participating actively in discussions related to cybersecurity, child online protection, quantum AI, digital public infrastructure, trying to engage constructively with governments and other stakeholders to ensure that their concerns are addressed within the remit of the ITU, and the ITU mandate is not expanded to the Internet via these additional emerging technology items.

And to wrap up, in a few weeks' time, ISOC will publish the ITU plenipotentiary background paper, which will explain more about our concerns, what we are following, what ITU plenipotentiary is, and why you should care. So, watch this space. It will be on our website. And shortly before the plenipotentiary itself, we will analyze all the resolutions, proposals as we do, and publish the matrix of resolutions for anybody who doesn't have time, but still wants to have an idea what to follow and what's going on.

Thank you very much. And if anybody has any questions, feel free to follow up with me. I'm still here. I'm still around until the end of today. Did I exceed my time?

ELENA PLEXIDA Pierre.

PIERRE BONIS Thank you, Tatiana. And thank you, Janis. Just to add, if anyone has questions, of course, there's Janis and Tatiana, but I want to say that Lucien Castex is one of the vice chairs of the ITU Working Group on Internet Related Resolution, which illustrates what Tatiana said about the European region, because everyone knows that Lucien is working for a ccTLD and not for the French government, but has been accepted to represent the French government in this ITU Council. So, you can also relate to him if you have any questions about these resolutions. Thank you.

ELENA PLEXIDA Thank you, Pierre. Yes, and it's exactly like that. So, the internet resolutions are the most relevant things to this community. Of course, Tatiana expanded to many other items, because as Tatiana said, ISOC's mandate is much broader. As regards to European cooperation, we are super thankful to France, the Netherlands, and the UK, because they are the ones who are really leading on these topics.

They are experts, they know, and they're leading in a very good way. Tatiana said Europe is the least problematic region. I will say, actually, it's the most helpful, the most supportive region entirely. Yeah. So, things are looking very good from the European side, at least. And yes, we discussed a lot about legislative initiatives and everything else that's going on in Europe.

But one thing to be said is, when we get to the global states, global settings, Europe says and does all the right things with respect to the support of the multi-stakeholder model, et cetera. And I have another shameless plug, Janis also has the plug on the ITU and the plenipotentiary. Is there any other comment please on the ITU?

ADAM PEAKE Going once, going twice.

ELENA PLEXIDA Back to you, Janis, for the WIS+20 Implementation.

ADAM PEAKE [CROSSTALK] is online.

JANIS KARKLINS Okay. Thank you. Janis Karklins again. On the WSIS+20, the conference ended with the consensual agreement which took form of UNGA resolution. And from ICANN's perspective, there were three good things in it. The first was the acknowledgement of multi-stakeholder model of internet governance, the

acknowledgement of technical community as a separate stakeholder or distinct stakeholder group.

And then the third one was establishment of IGF as a permanent forum within the United Nations system. On top of it, we got also a brownie and that was a very good language on multilingualism and then IDNs. So, of course, now all this needs to be implemented and transposed in different processes. The first meeting of Commission Science and Technology for Development after the UN General Assembly took place already in April this year in Geneva.

Some of the presidents in this room participated in the negotiations. There were three days of very, very solid negotiations of the text. Ultimately, text is good and reflects the language of WSIS+20. So, now on IGF. IGF is slightly delayed this year because the announcement of the Multistakeholder Advisory Group was delayed for three months more or less and the preparations are just starting.

As a result, probably we cannot expect very big progress in terms of reforms of IGF and processes within the IGF this year, but we need to roll up sleeves for next year. So, the first informal consultations on the IGF program will take place June 24-26 during the first IGF MAG meeting in Nairobi, Kenya, where the IGF itself will take place in December, between 14 and 18 of December, almost like a Christmas present.

What would be important from the European stakeholders is to come up with a very strong message that IGF needs to become

more efficient, more inclusive, and bring new people in the community. Otherwise, it may become stagnant. So, in this respect, I think that the coordination among different stakeholders would be useful, and participation in the open consultations is absolutely a must.

The last piece of information, the chair of the MAG comes from a technical community, that is Jennifer Chung from DotAsia, and we need to support her in every possible and impossible way. Thank you.

ELENA PLEXIDA Thank you, Janis. We will pass it on to Sophia online.

SOPHIA LONGWE Hello, everyone. Thank you very much. My name is Sophia and I work for Wikimedia Germany. And I was actually also an ex-Gener last year at ICANN83. So very happy to be back in the Europe space. I represent civil society on the IGF MAG that was recently appointed.

And also, I can only basically support what Janis just said, that the WSIS+20 outcome is a huge success, that we have this opportunity with a permanent IGF mandate, and that now it's really the time for all of us to engage, and especially for the technical community, to really show that multistakeholder governance works. And I can only highly encourage you to participate in the open consultations that will happen in June in Nairobi, but you can also join online.

I'm also copy-pasting the link to register in the chat. And otherwise, we're also at the moment evaluating the intersessional work. So, there are policy networks and also dynamic coalitions. The dynamic coalitions are self-organized. So, you can also just be on mailing lists there and participate. And then the policy networks will be endorsed by the MAG.

And then also, I think a huge nice thing about the WSIS+20 outcome are that national, regional and youth initiatives were recognized. So, also, highly encourage everyone to participate there. For example, EuroDIG, so the European dialogue just finished. I think Sandra will also say something later. But also, for example, national initiatives like I think the Swiss IGF will happen on June 21st. The German one September 9th. So, I think that's really great.

And then one important thing is genuinely to maybe also link more internet governance conversations to what's going on in the AI space. So, maybe also the global dialogue on AI governance that will take place in July 6th and 7th parallel to the WSIS Forum and the ITU AI for Good in Geneva. So, I think it's really important that we kind of connect all of those conversations.

And yeah, I can just encourage everyone to engage and also always happy to answer questions. You can also reach me via email and happy to discuss anything IGF, anything national regional initiatives and also the sensational work and also the meeting in Nairobi. And I will be really looking forward to that. Thank you.

ELENA PLEXIDA Thank you, Sophia. Any comments from anyone? Yeah, of course not. Now we're all happy. I was about to joke, say now we're happy with the outcome.

PIERRE BONIS Good work and good luck.

CHRIS MONDINI Hi, it's Chris Mondini again. I will echo what Sophia said about recognizing that IGF is more than just the one annual global meeting. It's a movement. It's a global movement, and it manifests itself in national and regional and youth activities as well. And so, as she encouraged us, now is really the time to participate and to get involved.

Elena has made the report the point repeatedly that ICANN has a very limited mandate and some of the technical communities that are represented here have a very limited technical mandate and point of view.

But at the IGF, there are many, many internet related topics that get discussed, and having a representative of this technical community in the room for those conversations is very important to be able to make that distinction, to be able to help people understand the layers of the internet and where the hot button, buzzword, sexy issues of the day are very interesting and get a lot of attention, but at its base and its foundation, an understanding of

how this model and how our communities work and how we administer these key resources is really important. So, all of you can be emissaries of that message. Thanks.

ADAM PEAKE

Thanks, Chris. I think it's a very good point. We have a lot of national IGFs and there will be a regional IGF for the southern and eastern European region. I hope Sandra will be able to join us, who is the Secretary General for EuroDIG, which happened earlier in May. And we have Elisha here, who's organizing the UK IGF. I think Declan McDermott might be here for the Ireland IGF.

You will find a national IGF in your country, your region. Please try to participate. It's how we make our voices heard in this important process. So, thank you. I mentioned Ireland, so, I think the next point is to pass along to Eoin. Eoin Carney is one of our GAC representatives and his ministry is also somewhat involved in the presidency that Ireland takes up in a few days, I think. So, thank you. Over to you, Eoin.

EOIN CARNEY

Thank you very much, Adam, and thanks for organizing this session. It's been really useful, actually, for us. And, yeah, I'll try to cut this a bit short because of the time, but luckily, the timing of this, we actually just published our priorities online yesterday. So, I think if you go to ireland2026.eu, you can read in more detail about some of these things that I'm going to talk about.

So, for those that aren't aware, Ireland will have the presidency of the EU from July till December, so just starting in a few weeks. At a kind of high level, there'll be 22 informal ministerial meetings, including the telecoms informal in October. There'll be over 250 events, over 30,000 people coming to Ireland for the presidency. The kind of overarching priorities for Ireland are competitiveness, values, and security.

And going into the telecom sector, I won't go into too much detail here. I think a lot of it's been covered already especially the Digital Networks Act. But another kind of priority for Ireland that hasn't really been mentioned is subsea cable resilience. So, that's going to be something that we're going to focus on in our presidency, advocate for increasing investment in subsea telecoms connectivity and generally diversifying the cable routes across Europe.

Also, the digital simplification package, we expect that this will be advanced during our presidency, where we will need to strike an appropriate balance between simplification and the removal of unnecessary duplication, whilst also retaining strong consumer protections. Ireland recognizes that a more coherent and effective digital rulebook is a critical step to boost competitiveness.

As well, there's the mobile satellite services, the two gigahertz frequency band will chair discussions around a decision for the future use of mobile satellite services in Europe. The European business wallet trilogues will be coming to an end. And then finally,

just as well, just to say that the ITU is definitely on our radar as a major milestone for the Internet governance landscape.

And we view the WISIS review outcome document as an important template for basically leading the work at the ITU, in particular the reaffirmation of the critical role of an inclusive multistakeholder approach to internet standards and resources, and then also the recognition of the importance of human-centric and human rights-based approaches to ICTs. And then just very briefly finally to mention a few of the events.

Again, there's many events, but to flag a couple here, there's going to be a child online safety forum in September, which is particularly focusing on youth participation in that discussion. And then there'll be an international AI summit in October, which I think kicks off a month-long EU AI innovation initiative. And then also, as was just mentioned, I think it's important to call out as well the national IGF in November which is also supported by ISOC and ICANN.

So, thank you very much for the support on that and organized by our multistakeholder community as Adam mentioned. Declan who's around somewhere I think at the conference. So, yeah, I'll leave it at that. If you have any more questions about the priorities, feel free to come up to me. Thanks again.

ADAM PEAKE

Thanks, Eoin. We're really up against time. One minute over. Sandra, I do see you online. I'm sorry, I missed where you were. EuroDIG, all of the reports that I've heard have been an exceptional conference this year taking place in Brussels. And could you please just tell us for just literally two minutes, otherwise the tech support will kill us because we have to switch everything off. And thank you so much for your patience and my apologies. Thanks.

SANDRA HOFERICHTER

Yeah, thank you, Adam. Doing this in two minutes is really a challenge, and also I do not know if there are any slides visible in the room that I've sent earlier.

ADAM PEAKE

Yes, they are.

SANDRA HOFERICHTER

Okay. So, if you move on to the second slide, this is something that I would like to highlight, which was the cooperation between EURid and the European Commission which organized a EuroDIG together with us. And this was really a very fruitful cooperation. And for instance, that led to the participation of the Executive Vice President, Henna Virkkunen. I'm moving to the next slide with her on the picture.

She emphasized the role of Europe, and that it will be shaped by choices by governance and by cooperation and that we have to keep up the internet as a transformative force. Some facts and

figures are on slide number four, if you would move to that one. Our cooperation with EURid and the Commission led to a record number of registrations.

We received overall over a thousand registrations and that resulted in 450 participants on site and another 215 that joined online. And if you move quickly to the next slide, slide number five, you will see some numbers. Here, I would just like to highlight that the lower right graphic, that the number of first-timers that attended EuroDIG for the first time, was significantly higher.

Usually, it's about half of the participants. This time it was even 70%, and that plays definitely into the efforts of EURid doing a really good marketing campaign for the combined effort of the 20th anniversary of the EuroDIG. And on the program, it was a bit shorter. That is on the next slide, number six. It was a bit shorter, two days only.

ADAM PEAKE

May I interrupt? I think the slide that we really are out of time, and if maybe you could jump to slide number nine which is focus areas, I think that's the one where the content of EuroDIG this year was exceptional. And if you would just quickly jump onto that one beginning, it's focus areas, and then WSIS+20. That's a highlight. And I'm really sorry, Sandra, we're up against lunch, but also, we have technical requirements, and it's not fair of me to ask the

support to continue. So, sincere apologies. Let's have a look at this one, please.

SANDRA HOFERICHTER

Slide number five highlights the focus areas. Of course, WSIS+20 was a focus area since EuroDIG was the first regional IGF after the review. And also, digital sovereignty was one of the topics, as well as AI and public services and some technical issues that you can see on the slide as well. What is not on the slide, but what was discussed a little bit earlier on digital sovereignty.

If time permits, I would just like to share a little bit of the messages that came out of this. And on the following slide number 10, you see a QR code that leads you directly to all messages from Brussels. But on digital sovereignty, as said earlier, it was defined as resilient openness and strategic autonomy leveraging Europe's strengths and not about isolation protectionism, fragmentation of global and digital cooperation.

It was noted that Europe's resilience on external digital technology creates strategic vulnerabilities, especially for democratic values, and that Europe must maintain its internet openness, technological choice, and adherence to open standards and interoperability while upholding human rights and multi-stakeholder values.

Of course, we must invest in Europe in trusted platforms, chip semiconductors, cloud AI and open data. Several speakers

emphasized that open source and interoperability are in their focus, in particular in public services. Balanced regulations and common European frameworks are other actions that you can find if you go through the messages in more detail.

And if you would like to have even more information, the transcripts, the videos, and also detailed session reports are on our EuroDIG wiki, and you will find the link to the EuroDIG wiki on the last slide. Thank you very much.

ADAM PEAKE

Thank you, Sandra. And again, my apologies. Maeva, if you just jump to the Google Doc, please. Thank you, everybody, for participating. Thanks to Elena and her team, Maeva Devoto and Dimitris and everybody else's help with this. We will have a Europe Space in -- it's somewhere down at the bottom here, I think -- we will have a Europe space at ICANN88 in Lisbon.

We had a particular format and topics for today. If you would like to suggest anything, what should we focus on? Did this work for you? Of course, we ran out of time, so we need a five-hour meeting, but please send me email and we will try and develop an agenda and format that works for all of you because it's meant to be your meeting.

And thank you very much, everybody. Meeting is closed. I think we can finish the recording. Thank you. Thank you, everybody.

[END OF TRANSCRIPTION]