MICHELLE DESMYTER: Good morning, good afternoon, good evening and welcome to the first edition of 2022 of the monthly roundtable by EURALO on Tuesday the 1st of February 2022.

In the interest of time, we will not do a roll call, but all attendees' names will be noted on the Wiki agenda page after today's meeting. We will have English, French, Spanish and Russian interpretation on today's call.

A kind reminder to please speak clearly and slowly to allow for accurate interpretation and also please state your names every time you speak, not only for transcription purposes but also for the interpreters to identify you on the other language channels.

Thank you so much. I will now hand the meeting back over to Sébastien Bachollet, chair of the EURALO.

SÉBASTIEN BACHOLLET: Thank you very much, Michelle. Thank you for the ones who are already there. I know that it's already recorded, but it's also sent to other channel. I know that my colleuage, chair of NARALO, Eduardo Diaz is already doing something on Facebook. So that's great.

Thank you for our two speakers. It's the first one of the year, we try something a little bit different, but we were very happy to have the agreement of Chris from RIPE NCC—RIPE has a memorandum of understanding with EURALO—and we are happy to have one ALS coming and speaking to this call. I hope that others will be ready to give a presentation during our next meeting.

I know that Olivier is not just wishing all of us a happy new lunar new year but is also going to have a full dinner and a full night about that. Therefore, he may be not participating to the whole meeting. That's a shame. But if he's not here, I will try to take the floor when he will leave to help for the moderation of this call.

Once again, thank you for joining this monthly roundtable run by EURALO. And Olivier, I'll give you the floor.

OLIVIER CRÉPIN-LEBLOND: Thank you very much, Sébastien. Welcome to this month's roundtable. Today we have two people that will be joining us. First, we'll have a presentation by Chris Buckridge who has been with RIPE NCC, used to be called Réseaux IP Européens. That's the regional Internet registry, the organization that distributes Internet Protocol addresses—IP addresses—those numbers that every computer needs to be able to connect to the Internet.

And the regional Internet registry for Europe is RIPE. There are five regions in the world. RIPE is one of them, and they've done this job ever since the very beginnings of the Internet. Chris is going to speak to us about what's happening at RIPE, the issues of global strategic engagement, and he has been pretty much steering part of RIPE's strategy for a number of years. So do not feel shy to ask him any question about RIPE and about what's going on in Europe and with regards to not just IP addressing but pretty much Internet governance in general. He has been representing RIPE at ICANN For quite some time, but also elsewhere following the whole Internet governance fora, etc. And we also have to note that he's part of the global equal

multistakeholder band. Always important, and that certainly makes him a very worthwhile person to talk to right now.

So that's one person. The second person is Frederic Taes who is from Internet Society Belgium chapter, and he will be able to speak to us about the recent developments, again speaking about the laws on encryption and on the whole diversity mandate that the Internet has. And of course, he follows the whole motto, the Internet is for everyone.

Let's start with Chris, and as Sébastien said, I'm not sure if I can stay the whole length of the call. Without any further ado, Chris Buckridge.

CHRIS BUCKRIDGE: Thank you very much for that introduction, Olivier. Thank you to EURALO for the invitation to be here today and to speak in this. I think this is probably one of the first RIPE NCC updates that we're giving this year. I think like a few others, we probably pushed back a couple of our usual January events in the hope that we might be able to get back to physical meetings, but it seems that's not to be the case. So we're still doing everything remotely.

But aside from the fact that we're not actually having our physical meetings, I think this is actually a really interesting and complex and somewhat unpredictable time for the RIPE NCC and the RIR system in general, and I think it makes it a really interesting moment to do a bit of an update, not only on the Internet governance and regulatory scene which I'll get to later in the presentation but also about the RIPE NCC itself. About where the RIR communities fit into the current Internet governance scheme and how we see that developing.

Sébastien's already had a look through my slides and noted I don't mention ICANN too much here. And it's an interesting point, actually, and something I hadn't perhaps realized myself. I do think, at the outset here, there's a huge amount of value in the crosspollination and making sure this communication and contact is happening between the RIR communities and the ICANN communities. I think that's a given and definitely, as we engage with other stakeholders, really important.

I do, though, note that I wonder if then perhaps note that we don't see as much operational crossover as we once did. I think what we see now is a much less active role for the IANA functions now that IPv4 has essentially exhausted from the global pool, the IPv6 and ASN pools are much less dynamic or complicated to manage, so IANA is a very straightforward process from the numbers community side. So yeah, keeping that relationship alive and dynamic is definitely a challenge and something that we need to discuss and look at how that can work.

But I'm going to jump in here. Next slide, please. The RIPE NCC is at quite an interesting moment right now because in the second half of last year, we did a process to develop a five-year strategy. So obviously, this is not something we do every year. But it was something that looks ahead to the next five years, helps us to understand, as the RIPE NCC, where we fit into this Internet ecosystem, and then to develop the more specific plans that would come on a yearly basis and develop over time. Next slide, please.

This was presented to our last RIPE meeting which took place in November, and we had some further input for the community. I think

the Board has now approved the final version in spirit, if not in the letter. I'm not sure if that's coming at a future meeting.

And I don't want to get too much into the details, but I think it's really useful to share some of what the high-level strategic objectives were for the RIPE NCC. And it really highlights a couple of points that I think are worth making.

These, I think, are not necessarily in order of priority, but there's perhaps some priority. And I think it's notable that the top priority here for the RIPE NCC is to support an open, inclusive and engaged RIPE community. It's a really important recognition that the legitimacy of the RIPE NCC comes from that community process, from the fact that we are guided and bound by community-developed policies rather than operating off our own badge or sort of at the behest of any other specific members or stakeholders.

So then second—and as I say, there's no priority, but coming in second is operate a trusted, efficient, accurate and resilient registry. And that's the role that we're probably most known for in many cases, running the regional Internet registry of IP resources. And running that registry to be trusted, efficient, accurate and resilient is not quite the same task that it was in years past. I'll get into that more deeply later in the presentation.

Third is to enable our members and community to operate one secure, stable, resilient global Internet. That's a really key one in talking to ICANN and the ICANN community, I think, because that single global Internet, maintaining that single global Internet is a common cause, a

common theme that runs through both RIPE community discussion and ICANN discussion.

Fourth is maintaining a stable organization with a robust governance structure. And this is something that's a challenge for all multi-stakeholder organizations these days. ICANN went through, obviously a very big process a number of years back in relation to accountability around the IANA stewardship transition, that is an ongoing process.

The RIPE NCC is also going through those kinds of processes. We've had a RIPE accountability taskforce recently, we're looking to strengthen our own accountability processes, and reporting to our membership and community. So that's really important.

And then fifth is attracting engaged, competent and diverse staff. That's a bit more of an internal goal. But I think also a very interesting one, particularly in this time of COVID, in this time of less ease of movement around the world. So that's worth looking at.

I want to jump back into number three. Next slide, please. Because this strategy document which there's a link on in the first page, and I'll share the link in the chat later on, is actually broken down into specific points. And there's a couple of interesting ones here under three.

One is coming back, well, a couple of them are coming back to different services. First one to do with RPKI. So that's a resource, public key infrastructure, to do with securing Internet resource registrations. Second is supporting the global naming system through operation of

K-root and DNS services. That's something where there is obviously a lot of overlap with the ICANN community.

And then it goes into a few other points in terms of being a center of excellence for data, measurements and tools, and supporting innovation and evolution through good of the Internet initiatives. So those are also very important. Can we jump to the next slide, please?

So the fourth point here on maintaining a stable organization with robust governance structure, one is to ensure the organization's stability and final financial strength. And that's something I'm going to talk a little bit more about in a second, because again, it's not the same as it was a few years back, it has changed.

And then point to there, which I think is really important, be resilient in the face of political, legislative and regulatory changes. This is something that the ICANN community is very familiar with, and something that the RIR communities, not just the RIPE NCC, but others in their respective regions are also facing. And it's why I'll devote the second part of this presentation to digging a little more deeply there.

Just the one other thing that I'd point is protect the joint Internet number registry as developed by the Internet community. This is really an RIR system where the five RIRs work together very closely. And one of the things that the NRO Executive Council, which is made up of the five CEOs, is doing right now is actually a strategic retreat and strategic development forward looking project to do something similar to this and to make sure that the our system itself is resilient, is strong, and is ready to face the challenges that are coming at us from various directions.

If we can jump to next slide. And I've done this a little bit backwards, because in the document, it talks about the factors that drive the strategy, and then the strategy. I wanted to hold off on the factors here, because I wanted to highlight the points that you can see in the arrows and the colors here. It's quite a list of factors.

We have a lot going on, a lot of different factors that are affecting how the RIPE NCC operates, but there are kind of two themes that I see emerging in a number of these. The first is politics and regulation. With the first bullet there is political issues. It's talking about sanctions, talking about our ability to engage, talking about financial impact because of work with the banks.

We're seeing legislative and regulatory issues in the EU, how that affects us, the potential regulation regarding digital taxation, efforts to destabilize the RIPE NCC Or the RIR system. So coming at us in a range of different ways.

The other key point is that our actual community membership, the RIPE community itself, which is a membership plus any other interested stakeholders, is also changing. It's also developing, we're seeing different incentives, different kinds of actors. We have IP address brokers now taking a very active role in policy development, that's actually changing the way that our community works. And it's making us look more closely at how is policy made, what are the sort of mitigations against potential capture or ensuring inclusivity and diversity in the RIPE community.

And so we see a few different things that we see in terms of factors, the effect of consolidation, in terms of membership growth and income, we

see development of market for Internet number resources, divergence and conflicting interests of various groups in the membership and community. And then also the need to ensure diversity in that community. So if we can jump to the next slide, please, thank you.

Going back from the five year strategy to look at what sort of our managing director has outlined for look into 2022. Goals, obviously maintaining accurate registry, strengthening RPKI and RIPE database infrastructure. So that's one to really take note of because RPKI has the potential to be quite a bit of a game changer if there is large uptake in relation to Internet number registrations.

Security, risk management and compliance. And I'll talk a little bit more about that shortly. Effective outreach and engagement. And that's very clear in relation to public policy. And then supporting the RIR system and wider Internet governance ecosystem while maintaining an effective, sustainable organization.

So that's kind of where I wanted to set the scene, I guess. Now, I want to just go into a couple of the, what we actually see happening in relation to the RIPE NCC. If we can jump to the next slide, please.

This one I'm sharing just because it's an interesting trend we see. This is membership growth in the RIPE NCC. And so it sort of shows you the number of new [inaudible] members to join per month. Predictably, as we got to IPv4 run out in 2019, we saw that growth really skyrocket. There were a lot of people getting in, becoming members of the RIPE NCC so that they could get their last slash 22 block of IPv4 address space.

Still predictably, that fell off afterwards. We sort of saw a real drop in the number of new membership memberships that people were opening. Interesting, we've seen it start to grow again. And that's due to—we hope lots of people adopting IPv6 and getting IPv6 allocations. It's not that. And if you jump to the next slide, I'll show you here.

What we are seeing is an increase in the number of transfers, the IPv4 transfer market. So to actually buy an IPv4 address block from someone else, you need to set up a RIPE NCC account so that the register the transfer of registration can be placed in the RIPE database. Now what we've seen over the last few years, and you can see from this chart, sort of going back to 2018, is that the number of transfers, the RIPE NCC's been asked to do. So essentially transactions, although the RIPE NCC doesn't have anything to do with the financial side of that transactions, just to transfer registration, but that's significantly growing. We've seen that increase. and that's one of the factors that I say is driving change in the community because as IPv4 addresses become assets or become things that can be bought and sold, that increases the incentive for fraud. It means there's a necessity for the RIPE NCC and the other RIRs to focus a lot more on due diligence making sure that everything is above board and that all of the documentation is correct. Throw in issues of privacy and not being able to hang on to IDs for too long due to GDPR, the process of doing this has become much more intense. So that's something that we're working with, also looking at sort of automation possibilities and how we can work that into our systems. But ensuring that we're actually doing this in a way that the community expects and trusts us to is a real challenge and takes a lot of work that we're currently looking at doing.

Now, that's further complicated by—if we go to my next slide here—dealing with sanctions. So one of the real challenges that the RIPE NCC has faced over the last year, two years, has been the fact that we have had to comply with the EU sanctions regime. And so these are sanctions that the EU has placed on individuals in a number of different countries, including Syria, Iran, Belarus, Russia, and a few others.

Now, we a few years ago, after some further investigation found that actually yes, we did need to take action on the sanctions. What we found after sort of working with lawyers, working with others in the field, is that there's a need, if an individual is under sanctions, or if an organization is associated with that individual, the resources have to be frozen in the RIPE database so they can't sell them, they can't get more resources, their registration is frozen.

That doesn't stop them using the resources they have. So that's a useful point. But it is really an existential challenge to the regional Internet registry model, because we are a registry for a service region of 76 countries. And yet, we have to comply with the sanctions regime of a single country, in this case, the Netherlands, which is where we're based, and the Netherlands is obliged to comply with EU sanctions regulations, because they're in the EU.

So we've been putting an awful lot of work into making sure that we're compliant here, making sure that we're monitoring membership against EU sanctions. That's something that we absolutely have to do. And we're trying to be, obviously, as transparent with our membership and our community as possible. We now have quarterly sanctions transparency

reports, and there's a link there where you can find those, I think we've done two so far.

Adding yet another layer of complication to this is the fact that while we're required to abide by EU sanctions, the banks that we deal with, including banks in the Netherlands, have an even higher level because they're also having to comply with OFAC sanctions. So the sanctions that are applied in the US. So that has meant that there's been a lot of discussion with our banks in terms of actually being able to continue doing business, because—and if you've seen the news, you might have seen a number of Dutch banks got into trouble relatively recently for not abiding by sanctions in the strictest sense. So now there is a real heightened sense of risk and compliance for financial institutions in the Netherlands. So this is all stuff that we're working through, dealing with.

But the other point is, as I say, this poses a really significant challenge to the multi stakeholder model of how we manage Internet governance. So what might also be on our agenda and what we're sort of working with some people to look at during is campaign, or at least some work to engage with the EU, on how to refine those sanctions regimes to perhaps better reflect the special kind of role that an organization like the RIPE NCC has, and hopefully, allow it to operate in its multi stakeholder model, rather than be bound by sanctions in this way.

So if we can keep moving forward here to the next slide, and I'll sort of segue here and I've got five minutes left to speak, and I might go a little bit over that.

Segueing into the more general public policy space here. And it really is a very significant space for the RIPE NCC. It's one of the big priorities

that we have these days, is making sure that we're engaging with political issues and able to engage effectively.

Now, we are based in the EU, so the EU is obviously quite a big focus of our attention. Also, because the EU itself, the commission, but also other institutional actors there have become very proactive in their efforts to regulate the Internet and regulate the Internet in Europe, and if beyond, then so be it.

One of the big things that we've been dealing with recently is the NIS2, which is the Network and Information Security Directive. And that's been particularly in relation to the route service system. And so this is something we've also obviously worked with ICANN on, also NetNod as another operator of a root server, to ensure that the Commission's original draft, which would have brought operators of root servers into the NIS2 regulation as operators of critical services, is not covered there, because essentially, that would be the EU regulating global root server system. And it would cause many problems, I think, not least of which is that it would encourage others around the world to also bring the root server system into their regulatory framework, the legal framework, which would make the operation of the current root server system very difficult.

At the same time, then, so just to round out NIS2, that's currently in final negotiations, trialog they call it, between the different actors in the EU, the parliament, the Council and the Commission. We're quite hopeful, we've found some receptive folks in particularly the Parliament and the Council on our arguments here. And they've both drafted alternatives that would remove the root server operators from scope. And so we're

waiting to see what the result of that is, but we're quite hopeful. And that's been due to some really good work and cooperation, I think across the technical community. And that's including working with ICANN, NetNod as I said, but also others in the DNS community.

There's been a lot else going on. And I'm not going to go too deeply into any of this. The Digital Services Act and Digital Markets Act as a package are doing a very significant and will have really significant impact on the Internet industry and communities. Data Governance Act is obviously something we're paying close attention to, as with eEvidence as a directive and a regulation there and ePrivacy, which will have an awful lot to do and potentially have quite an impact on us and how we work with members and with stakeholders in the EU.

Additionally—and I won't go into too much—DNS4EU has been a really big point of conversation in the last few weeks. And so this is the European Commission's proposal and now opened for bids to establish a European based public DNS resolver. There's a lot of open questions about that. It raises a lot of questions about the role of government, about the DNS system and the ecosystem around it. We actually did a webinar yesterday, which I'll post the link in the chat to the recording, but we had about 150 people, and some really good discussion about them. So it is really an interesting topic. And then also, the Cyber Resilience Act is going to be published later this year. And so we're waiting to see what that's likely to conclude and entail.

If we can jump to the next slide, please. Got a couple more. There's obviously a lot more to our public policy engagement than just the EU. And I've kind of just listed here a few of the different spaces were

working in. IGF, obviously, is at quite an interesting moment. And as of this year, I'm part of the IGF MAG, so I'm paying even closer attention to what's going on in the IGF. But we are sort of looking at that developing particularly in the coming few years, leading up to the WSIS plus 20 2025.

And we're also looking at the evolutions that are happening in relation to it with new actors in the UN, like a new tech envoy, possibly a new leadership panel that's been talked about. I think we expect to see some things change there. How they'll change we're not sure.

The ITU, International Telecommunication Union is also going through a very busy year this year. Unlike some other organizations, they actually postponed many of their big events and conferences over the last two years, which means that this year they actually have three really significant conferences, the WTSA, the WTDC, and the plenipotentiary, which will be a lot of work for a lot of people. But it's also a slightly risky situation, if you're looking at keeping track of everything that might be coming through, keeping track of the sort of small incremental changes that could lead to expansion of the ITU's remit, or sort of stepping more into Internet governance areas. And that's how the ITU works, through those sort of small incremental changes. So it is a time for people to be paying attention to what's going on there.

And then I won't go through the rest of these. But yeah, working with the OECD, recently did some work on both DNS abuse and RPKI routing Security. Council of Europe, which is doing a lot at the moment, particularly around the Budapest convention, and there was some discussions of that in the EU parliament yesterday, League of Arab

States, and of course, individual governments are doing an awful lot in this space in terms of new Internet regulation. Russia, there is an awful lot going on there, which is very interesting, if you dig into it. I know ICANN's own people have published some really interesting reports on that. So it's worth having a look at.

If we can jump to the next slide, kind of my last substantive one. And it's really just to say the takeaways here is that both global digital policy and Internet governance is really increasingly complex. We're seeing a lot of different actors doing a lot of different things, planes intersecting, and keeping track of it is both important, but increasingly difficult. We do see a lot of governments, particularly I guess, the Western democracies, I guess you'd say, referencing that principle of maintaining an unfragmented Internet. It's not always something that's reflected in the regulatory or legislative initiatives they take. That fragmented approach to governance is still there. And by fragmenting the public policy landscape and ecosystem, that also risks a fragmented Internet.

The multi stakeholder model really remains our best defense against that fragmented approach, best effort to ensure at least some level of alignment to maintain a single global Internet. But the multi stakeholder models require multi stakeholder engagement. And that's, particularly after two years of no meetings and Zoom calls, I think is a real challenge, not just for the RIRs, not just for the technical community, really everyone is faced with that challenge. Something we need to work on.

I'm going to go through two final sides very quickly, just because I think for this community, it was worthwhile highlighting. One is the RIPE NCC community project fund. You can read the slide yourself, it's a 250,000€

fund that we give out each year for projects done for the good of the Internet. Around midyear, June is when the call for applications goes out. So I really, really encourage you to follow that if you're doing work that could be described as for the good of the Internet, and could use an additional funding.

And then to the next slide, please. Last one here is we also have eLearning platforms, and I've included some links there, it's even a QR code. But this is something that might be useful, I think, for this community, where we're sort of expanding our range of eLearning courses. And if everyone's sitting behind their computers, on Zoom calls, this is the time to jump in and do some of that. So yeah, let me know, please reach out if you've got any questions about that.

And that was the end of my presentation. So I'm more than happy to take any questions or just discuss in general. I saw there was something some comments in the chat, but I didn't have a chance to read them.

OLIVIER CRÉPIN-LEBLOND: Yeah, thank you very much for this, Chris. And thank you for this very interesting presentation. Well, we're now going to open the floor for questions. But in the meantime, while people gather their thoughts, because you've included a lot of things in your presentation, I should—and I didn't say it at the beginning, but RIPE has a an MoU, memorandum of understanding for collaboration with the EURALO. We're particularly happy about this. We have had some instances of EURALO members go to RIPE meetings in the past, but this is the first

time I think that we actually invite someone from RIPE to come to our virtual home.

CHRIS BUCKRIDGE: I think I've been before, Olivier.

OLIVIER CRÉPIN-LEBLOND: You did, yeah. I think it was in person, wasn't it? Atan ICANN meeting. The first time we see you on the screen. And of course, It's been quite some time since, as you mentioned, we've been far away from each other for quite some time on this.

Just two quick questions. One was to do with the relationship between RIPE, and actually the regional Internet registries and ICANN, I know that you do have some people that are—I've noticed that our newcomers and some fellows. [inaudible] relationship between the Address Supporting Organization, the Number Resource Organization and the regional Internet registries, briefly, in 30-second tweet.

SÉBASTIEN BACHOLLET: Just before Chris, you jump to this question, I just wanted to tell you that I put the link, when you were talking about any documents, therefore you don't need to do it again. I hope that I didn't make any mistake, but I have done the job. Thank you.

CHRIS BUCKRIDGE: Thank you very much, Sébastien. Olivier, I can try and answer that quickly. So the Address Supporting Organization is one of the key

supporting organizations in ICANN. The NRO is the Number Resource organization, which is the five RIRs working together, it's an umbrella organization for the five RIRs.

The NRO fills the role of the Address Supporting Organization. So in a sense, they're one and the same, but they are in a sense somewhat different. The five heads of the RIR registries, the CEOs, are the ASO—just called the ASO, but they're NRO EC. Then there is also the ASO Address Council, which is selected from three members from each of the five RIR communities. And so they also then undertake tasks such as I think, probably, most importantly these days, selecting the Board members for the ASO seats on the ICANN Board. And the real link there certainly, historically has been that ICANN runs the IANA functions, which is the global pool of the IP address registries. And yeah, as I say, I think as what are called iStar organizations, we have a lot of common ground and common purpose in engaging. That's that.

OLIVIER CRÉPIN-LEBLOND: And also a second quick one, which has to do with you've mentioned about the ITU and some countries that were looking at alternatives to the multistakeholder model, is there an increase in this in recent times?

CHRIS BUCKRIDGE: So what I've seen, I think, there are obviously countries who have long been pushing for a more centralized or more government control of Internet governance. What I think we're seeing is a shift in the Overton Window. And so the Overton Window is that concept of the window of opinion that is regarded as acceptable.

And I think what we've seen is that window of acceptable opinion and thought, shifting, where once you had a significant number of countries really buying the idea of okay, we need hands off regulation, there's no need for regulation of the Internet, let it grow, let it flourish. Even a lot of those countries, and this is, like I say the EU is perhaps the most active, or one of the most active legislatures we're seeing in regards to this are saying, "Okay, no, we need to regulate here."

Now to different degrees, we'll work with the multi stakeholder model, we'll work with the community, we'll open it up to consultation. But at the end of the day, what we're going to end up with is some more governmental control. I think, at the same time, what some of those other countries who have traditionally pushed it—I mean, Russia is I guess, the classic example, they've pushed very hard in the ITU. I think their arguments have been tempered a little and they have shifted closer to what others might find more acceptable. So I think that's the challenge for all of us, is that we do need to shift our technical community, iStar community mindset a little to, "Okay, there is a real need here, there is a real general understanding of there must be more regulation. How do we want to steer that? What influence do we want to have? And where do we want to end up?" Because I think we know where we don't want to end up. And we've spent a lot of years telling people where we don't want to end up. But now we need to actually come up with some more positive ways forward to solve this.

OLIVIER CRÉPIN-LEBLOND: Thank you, Chris. Let's go over to the queue. And first we have Sivasubramanian Muthusamy.

SIVASUBRAMANIAN MUTHUSAMY: Yes. You are mentioning that the proposal to include root servers contested and that EU is receptive to that, and also that ICANN or the Internet community is emphasizing that root servers should be out of the scope of legislation, especially the NIS2 directive. And likewise, the DNS4EU proposal takes shape. And if it is to be operated by the multi stakeholder community, which is probably the best way forward, shouldn't the Internet community emphasize that the DNS server should also be that the DNS resolvers should also be excluded from the scope of legislation? Do you see that happening?

CHRIS BUCKRIDGE: I think this is a really interesting discussion. And I think if you were in the webinar yesterday, there's obviously a very strong contingent, who are saying, this does not a role for government, we don't need to see the EU taking this role in relation to the DNS. I do think there's a really fundamental difference between the root server system and the ecosystem of resolvers, public resolvers that are out there. They're not multistakeholder for the most part. They're run by private organizations, Google, CloudFlare, but also by ISPs themselves, a lot of ISPs have their own resolvers.

So it all comes down to where is this going? Because I think if the EU, the European Commission wants to fund a new public resolver that abides by very specific rules, then so be it. If that then transitions to we're going to make users or operators in Europe use this resolver rather than any other resolver, that's a very different proposal. That's that. And that's I think where there's a lot of concern that that's where it

could end up. So yeah, it's definitely a discussion that's ongoing and as I said, we had a bit over an hour discussion about it yesterday, and I don't think we came anywhere near solving the question. And I think the EU Commission at least is powering ahead. They have this tender out. So I think that's likely to go forward.

OLIVIER CRÉPIN-LEBLOND: Very interesting. Thank you, Chris. Wolfgang Kleinwaechter is next.

WOLFGANG KLEINWAECHTER: Thank you, Chris, very much. And I also recognize like you that the political environment for Internet governance has changed dramatically in the last five years, which is not a surprise, because Internet governance isn't anymore a technical issue with some political implications. It's now a political issue with a technical component. So as Göran from ICANN tries to escape from this phenomenon to get pulled into the geostrategic conflict by introducing the language of technical Internet governance, so that he understands it, obviously as a layer and said, we have the ground layer which is very neutral, just technical issues. And on the higher layer, we have the political issue. So we had this discussion for many years. And I'm interested in your opinion, how do you see the interlinkage between the technical Internet governance and what I've called the political Internet governance? What would be the right—[inaudible] different [inaudible]. I think this is clear, but they are interlinked.

And a very final question. Just recently, the European Commission published a study on DNS abuse, which also has recognized the lack of

regulatory frameworks for the management of the DNS. Do you have any first comment on this new study, which was outsourced but it's managed now by Thomas de Haan, who was a former member of the GAC? Back to you, Chris, thank you.

CHRIS BUCKRIDGE: Yeah. Thank you, Wolfgang. On technical Internet governance, I think if your hope in defining and sticking to technical incident technical issues and technical Internet governance was to avoid the political sphere, that is not a working strategy. I think things like DNS4EU, things like the new IP discussion show that politics is coming at the technical layer of the standardization. The G7 commitment on standardization of last year, I think we're seeing political actors getting much more engaged when it comes to technical issues, which is, I think, a change from a few years back where political issues or the really sort of governance issues were in relation to content or relation to activities online. And we could sort of say, deal with that, leave the underlying infrastructure and underlying architecture alone. Now, we're sort of seeing that actually, both are happening.

So it's good to focus on the remit of organizations like ICANN, and RIPE NCC. But it's not going to prevent us from being dragged into political debates and discussions I don't think. in relation to the DNS abuse paper, I haven't had a chance to read it yet. It came out yesterday, and we didn't get any advance copies. And it's quite lengthy. So I don't really have any comment there.

What I wouldn't note is it’s interesting that this is almost parallel work coming out of the OECD, I think it's not declassified yet but it's certainly

in the final stages of drafting and approval. The OECD is another paper on DNS abuse. So it's interesting to see multiple venues and multiple organizations churning this stuff out. And that, I guess comes from a lot of interest in the ICANN community and the GAC there. But yet, keeping up with it all is going to be a challenge.

OLIVIER CRÉPIN-LEBLOND: Thank you, Chris. Unfortunately, I do have to drop off. There is an expression in English, which says your dinner is in the dog. And it might well be that my dinner is now in the tiger, since it's the Chinese year of the tiger, but I'll hand the floor over to Sébastien who will continue. And I think that Sébastien wants to also ask some question on this. Over to you, Sébastien. And thank you, and apologies for having to drop off.

SÉBASTIEN BACHOLLET: Thank you, Olivier, and have a good dinner. And on our behalf, please, eat a little bit more than usual, please. Thank you very much. Yes, Chris, I have a question for you. How RIP NCC deal with EU presidency in general? And maybe if you have something specific from the current one who is from France. Are there differences or not? And? Yeah, that's my question. Thank you, Chris.

CHRIS BUCKRIDGE: Thanks, Sébastien. And we absolutely pay attention to this. And we've tried to engage a little bit with some French government stakeholders, although not really at the sort of presidency level at this point. I think what we do see when any of the sort of the big EU states take the presidency, is they come in raring to go. I know the French have been sort of laying groundwork for this presidency for the last two years with

like consultations and work and setting things up. So I think they come in with a lot of momentum and drive to actually push through legislation, get things done.

I think that's going to mean NIS2 will be pushed through. Regardless, I know, they're very keen to get eEvidence sorted out, which, as I say, runs into some issues with Budapest convention. It's second additional protocol in terms of evidence sharing.

But yeah, it's a period in which we're definitely paying very close attention and trying to keep up with and engage with members of the parliament and the Commission and others as much as possible.

SÉBASTIEN BACHOLLET: Thank you very much, Chris. I know that you have members in France, but you know that you have other friends here and if you need some help with the discussion with the government, I am sure that both AFNIC, the French .fr registry and the chapter of Internet Society France could help if ...

CHRIS BUCKRIDGE: Thank you very much.

SÉBASTIEN BACHOLLET: Thank you very much. Chris, if you can stay with us, it would be great because maybe at the end, some people will say “Oh, I forgot to ask one question.” But anyhow, thank you very much for your presentation. I am sure that it was very interesting and very useful. Great. And now I will

give the floor to Frederic. And I am sure that it will be another type of presentation, but also very useful. Frederic, the floor is yours.

FREDERIC TAES: Thank you very much, Sébastien. Thank you also for Chris. By way of a small comment, I'm working regularly with [inaudible] community manager, [inaudible] society. And he has worked about 20 years for RIPE NCC. It's really good to have presentation today. And indeed, we are a big family with ICANN At-Large.

And today the topic I would like to present—and if you can show the slides, maybe—it's about DNS abuse. So the presentation, I will first explain the motivation, what motivates us to launch this project, to present [inaudible], then a small demonstration. And something I would like interactive with you is about the next steps and the challenges an d to get your feedback.

Project motivation first. So our ALS wanted to contribute to the global efforts for better Internet by offering a tool that provides the priorities of Internet users. And from survey we made, you know, understanding, the priorities are in order, the access to Internet. But as soon as you have access to the Internet, you are facing security, privacy, trust issues. And then content related and services which is coming afterwards.

Our ALS has rejuvenated since a couple of years now. We participate to ICANN 70 invited by you or by Sébastien. It was really a source of inspiration for us. I don't say that to just [inaudible] or whatever. But that's really the case. And what we learned, one of the key topics was about DNS abuse. And it was also confirmed by the latest, ICANN 72.

Just to remind what DNS abuse means. And we set definition. Basically, it's how to address malicious use of domain names, broadly referred to as domain name systems abuse. It's really the topic of the great interest and discussion we'd like to take today.

And DNS security threats include five broad categories of harmful activity: botnets, malware, pharming, phishing, and spam. I'm not going to go into the details to explain what it is, but you have more information on icann.org at DNS abuse.

The continued contribution is first is a complementary approach what exists already today, with a focus on the end user and tackle DNS abuse from an end user perspective. So it's not related to all things we are doing from network point of view or from organizations and other initiatives like DNSSEC. It's not that. it does not replace neither the initiatives to secure websites and e-mail servers. That remains a necessity, but it's really a complimentary approach focused on the end user.

And how it works, if I'm an Internet user, I am receiving a link as tonight, okay, you have a delivery [inaudible] please go on this platform to check delivery of your packet at home. If the website was suspicious, I can find out by checking my bowser, when the domain was created, the WHOIS owner of the domain, is the communication secure, etc. A few really key information in just one click.

It is a browser addon. It is free. Has data privacy by design, not any data is captured. It's also open source. The code is available to anyone. It's Copyleft license, so you can use the code, extend it, etc. And it has been already published on different platforms like Mozilla Firefox,

Google Chrome, Microsoft Edge. And Apple, we are in the process. It should be published pretty soon.

it's also multilingual by design and currently available English, French and Dutch. Just takes the language of the [inaudible]. Current version supports all gTLDs and a few ccTLDs. Thanks to ICANN, we have RDAP protocol, [inaudible] used by all gTDs that's really practical. It's not the case for country code top-level domains.

I can make a short demonstration how it's working. Here, just the two websites. I take Belgium.be, is that a commercial website or who is the owner of the website [inaudible] authorities or company? With some click, I can see that the domain is DNSSEC certified, it exists more than 25 years and it's owned by the first minister in Belgium. Also the security tools in recent version of TLS. The communications [inaudible] and the certificate is signed by [inaudible]. Just with one click.

And it's also the approach and the fact that people click there just to ask a question and think just a couple of seconds to think about, okay, is the website I'm visiting—can I trust this website?

I have another example. I don't have anything specially here about the owner, but on the right side of the screen, there is no known domain owner and even the communication is not secure. I can take the decision myself, can I trust this website or not?

Taking another example. I was looking for EURALO in Google. I go to website. You can see I come in AtLarge.icann.org. And the little v you see on the screen is DNSSEC, it's a signed one. When I ask people about DNSSEC, they don't know what it is and how to check if the domain

name—if the information they're receiving from DNS are signed eloquently. You can see that the website is existing since many years and the certificates also ICANN [inaudible].

Another example, it's also useful for domain name orders. Just take an example I know, it's Wayrich Edition, they took the domain name, but it was the communication agency that has registered the domain name. That's quite a common practice. But they have put themselves as domain owners. After a few years, the company filed for bankruptcy and it was taken over by another commercial entity and they were not able to get back their domain name.

And many different companies are not aware of the fact that the ownership of a domain is not because they pay for the domain that's their own. And this tool can also help to see who is the owner of the domain.

Also to be noticed, many fake websites, ecommerce websites. Here you can see that the look and feel is really quite the same. And we can observe that those fake websites, you order, you have huge rebate, 50%, but you never get the products you have ordered. And most of the time, the owner of the website is hidden behind the WHOIS privacy or behind a company, in this case in Bahamas.

Last example is about phishing and pharming. You can receive an email from noreply@apple.com with link to noreply-apple.com. But when you arrive there, it's not the official website of Apple, it's just a copy of the website and you can be abused that way. And you can see here the

website has been created a few days ago, not for really safe activity. Those are some examples here.

The next steps and challenge now. The next steps, we would like to engage users to play an active role in fighting DNS abuse. For example, by using this tool. And not only [inaudible] companies, organizations like ICANN, also users need to play an active role.

For [inaudible], we would like to have more ccTLDs onboarded. For example, France, I'm looking for contacts by the way. A third objective also to make it more efficient to convince companies that sharing Internet domain identity can only build trust. If you go on the website and you don't know who is the owner of the website, how can you trust if you don't know to whom you are talking? That's really difficult.

And who like also, these projects to promote DNS sec. For the tool itself, we have some ideas here, for the extensions. More languages, more ccTLDs, support for mobiles, email, also for the email phishing, finding similar names—typo squatting—and increase other directories [inaudible] reference but you can have other [inaudible] to take information about companies. For example, [inaudible] information.

That's it in a nutshell. I would like to invite you to go on IsTrust.org to install the plugins and to give you your feedback. And fair questions, fair feedback is always welcome. Thank you.

SÉBASTIEN BACHOLLET: Thank you very much, Frederic. Very interesting, I think. First, because it's done by a little structure—sorry, little, but a structure in the country

who is member of EURALO. And it's interesting that some of the discussion we had in ICANN made this idea to flourish. Now, I would like to open this discussion for questions. If there is no yet, maybe Frederic, you talk about where it is already possible to download. Is it the same for both Windows platform and Apple platform, or there is differences also here?

FREDERIC TAES: No, no, it's really the same. So it works for Windows or Mac. Both has been tested. A version for Safari will be shortly available, but it works with—we test with even other browsers [inaudible] also working with those browsers on Mac or Linux even has been tested. So Linux, Macintosh and Windows.

SÉBASTIEN BACHOLLET: Right, thank you very much. Next question. I have Sivasubramanian. Go ahead, please.

SIVASUBRAMANIAN MUTHUSAMY: IsTrust application should be retrieving information probably by API calls to the registries' database, registrars' database. Have you encountered any difficulties with regard to any registry or registrar with respect to access to even the public data of call by the API? And also, the second question is that if you had an overview of the data that you have retrieved so far, or the users have retrieved so far, do you see any data accuracy problem, any information accuracy problem with respect to location, name of the organization, etc.?

FREDERIC TAES: Okay, so there are three questions. So the first one, thanks to ICANN as I mentioned, we can use RDAP protocol. One important thing as we want to have this tool as Sébastien mentioned is developed by a small organization, we cannot have central servers. It is really a distributed architecture. So it is directly the plugin in the browser calling the different services. And the first one is IANA to know, okay, that's a .net or that's a [inaudible] for example. From where do I need to get the information? That's the first, but almost everything is managed from the browser itself.

And we had difficulties for country governments. For Belgium, we had the partnership with [inaudible] Belgium, there was a public API. For the Netherlands, we have good contacts. There is no uniformity there. So the first obstacle is that each country, we need to have a specific interface per country. And for some countries, there is no public API. It is possible to get information from online tools, but that's really heavy, heavy software then on the laptop of the end user, or the devices of the end users, and we don't want that. Sometimes it's even not possible.

So yeah, we had some technical difficulties. So that's why for France, for example, I would like to know, is there a public API or protocol that we can use from the browser to directly take the data? And for other countries like Germany, they don't want to have even this kind of service. So if you have a domain name in .de for Germany, there is no way to answer who is the owner of the website, the information I receive, it's only the owner that has the right to ask about his own data.

And the third question you had, can you go through your third question?

SIVASUBRAMANIAN MUTHUSAMY: I can't immediately recollect, but I have supplementary on the first part based on your answer. From what you've said, it looks like it's not like you have an application software and you launch the software, and then it starts working from day one. But you have to physically contact each and every registry, each and every country probably in the case of ccTLDs, and if it's for gTLDs, you will probably have to write to or reach out and establish relationship with each and every registry to make this work. Is that the case?

FREDERIC TAES: No, no, it's not the case. For gTLDs, 100% is already covered thanks to ICANN, because it is an obligation, a duty to have RDAP available and a standard protocol. And we are just using publicly available capability. So for the gTLDs, 100% is covered, but for the ccTLDs, for the country top level domains, each country can decide and offer another service and has different kinds of protocols.

SÉBASTIEN BACHOLLET: Thank you, Frederic, for your answer. We have a few questions in the chat. I will try to retrieve them and to tell you. We have one from Nabeel. “Nowadays, we are getting hoax messages by WhatsApp as well. Not anymore phishing site only. How can we do to protect the Internet end user?” I'm not sure that it's a question for you. But if you have any idea.

FREDERIC TAES: Yeah, but of course, as I mentioned, more for the immobile and more for the other kind of phishing. Yeah, that's something we would like to develop and also integrate with other tools. It can be Gmail, WhatsApp, or whatever. It's not currently today, but yeah, it's possible extension.

SÉBASTIEN BACHOLLET: In the future. Okay, great. We have a question. And I will ask them more generally. Some people in here already try to use it with Google, but she was not authorized to do so. I have done the same few days ago, then I didn't try again today. But with Chrome—or she's using Brave Chrome. I don't know which one I am using. But I got the same type of trouble. Do you have any idea what is happening and how we can solve that?

FREDERIC TAES: You can reach me, I can see what's the case. Is it on the company computer or your personal computer?

SÉBASTIEN BACHOLLET: I don't know for Avri, but I guess it's personal computer.

FREDERIC TAES: Okay, because in some companies, it's possible, of course, to block the installation of addons, or to have some security restrictions put in the configuration of the device that it’s not allowed to install software or to do several things. I was not informed about the Brave variant. Maybe it’s to be tested. But normally, it has been tested with different Chrome and

there was no issue. But you can reach me, istrust@isoc.be, or istrust.org, you can contact us and we will answer your issue. And there is a link GitHub to report the bugs or issues.

SÉBASTIEN BACHOLLET: Thank you, Frederic. And the last question for the moment in the chat, is it available as a plugin only format, or a web version of the tool could also be used to check the domain name?

FREDERIC TAES: It's only a browser extension today. If we have web version, it means that we need a server and we need to have the appropriate funding for the server etc. And that we wanted to avoid for different reasons, the cost, but also data privacy is really something important. I think it was one of the questions about the statistics. When you are using this tool, we don't know which websites you visit, it's only between you and the different websites and the different lookup systems or WHOIS or whatever, but the tool itself doesn't capture any personal information about websites. If it's public web service, it would be different. And then we need to take other measures to safeguard the data protection and privacy of visitors.

It was one of the issues with web of trust, it was the name, it was a service also, a community etc. But afterwards, they took all data to resell it to companies. Those visitors, those are the websites they're visiting, the data. And for this, with open source, yeah, it's more difficult with a central server on top of the cost issue.

SÉBASTIEN BACHOLLET: Thank you for that. And I have a question from Shiva. Go ahead, please.

SIVASUBRAMANIAN MUTHUSAMY: Yeah, I remember the question now. Based on the data that users have access so far to determine the validity of the domains, have you studied the degree of accuracy of registration data? Do you have an opinion about the level of accuracy of available registrant data?

FREDERIC TAES: Currently, from what we have observed, when there is data, [inaudible] accuracy. But there is not always data for some domain names, no data is available for domain names. That's a separate discussion, a good discussion, is how to reinforce the process to have accurate data, to control the data available in the differences directories. And so that's why we are also thinking about all the directories like the public search I mentioned. It's the repositories only for companies who have also paid service, like [inaudible] service, but it's a principle, we could interface with other source of information and to collect together everything together.

We have already two main sources of information here, the domain names but also the certificates. And we want to illustrate also with the certificate, there are two types of certificates, just the communication is secured or also you have a certificate with a name attached to the certificate. And most Internet users will not make the difference between the two. They just see, okay, it's HTTPS. Okay, it's secured. But

there is a difference. You can have a certificate, self-signed certificate, or signed by a third party. That we want also to illustrate with IsTrust.

SÉBASTIEN BACHOLLET: Thank you very much. Thank you all for your questions. Any last question? And if so, may I open also the floor for question back to Chris, if you want?

FREDERIC TAES: Yeah, I have also a call to volunteer, so a question myself. So if you have any issue, please contact me. If you want to make translated in another language, Spanish or whatever, do not hesitate to enrich the tool. It's a community effort, it's a publicly available tool and tool for and by the community.

SÉBASTIEN BACHOLLET: Thank you very much, Frederic, and I hope that people hear that it's open to help to develop the tool. Any other question? If not, I will not take more time. But I would like really very much to thank both Chris and Frederick. Two type of presentation, but some very interesting and useful both.

I hope that Frederic, you will be able to develop your tool with the help of others and that it will be a good success. I am sure that it could be interesting to have such presentation for more people. But at least now with a recording, our colleagues from other RALOs could go and try and use it and it will be great. It is the first time I guess that one At-Large structure come with a tool to be presented to us. And even if it's not to

present a tool, but your activities, please, members of the EURALO, feel free to reach out to staff or to myself and we will try to accommodate you for next time meeting for a presentation. It will be great.

Chris, thank you very much. I feel that it's a very useful exchange and discussion that we need to find a better way to communicate. But I think it was important to see where we are with the IP addresses in general.

One question to you, Chris. Can you tell us a little bit where our colleague from Africa are with the situation against the Chinese company who take them into big trouble? And I guess when we take one part of that family in trouble, I guess the whole family is in trouble. And I feel that even if I am not in the IP community, I feel very bad on what was happening there. If you can, if you have some, yeah, where we are with that and any information, if you wish.

CHRIS BUCKRIDGE: Sure. I probably don't have much more to say. Probably for those on the call who aren't familiar already with the situation, there is a very large member of AfriNIC who is suing AfriNIC the registry, because AfriNIC had frozen and then withdrawn the registration on their IP address resources, because the member was based in China and was using those addresses to connect VPN customers outside of Africa. And that was a rule and a policy that was set in place by the AfriNIC. community that that wasn't allowed. So the AfriNIC registry pulled it back.

There is a legal dispute going on, and that's still in process. I think there have been some small wins on the board for AfriNIC in the recent past, the last few months, but it's deep in the weeds of the Mauritian legal

system now. So there are many different aspects to the case. And it's ongoing. So we don't comment on it really. I mean, I think as you say, this is something that while we certainly don't want to interfere or get involved in AfriNIC's business there, it is something for the whole registry system to look at. For instance, at the ITU last month, the Council Working Group on the Internet [inaudible] submission actually highlighting both the RIPE NCC's challenges with sanctions and the AfriNIC legal situation as examples of why the Russians feel that these governance structures should be taken over by UN, by intergovernmental agencies.

So it is definitely of interest to the entire community. I think it also, as I mentioned a bit in my presentation, it's a reflection of that changing community. It's a reflection of the fact that IPv4 addresses are now really a very valuable asset, I think going up to something like 50 US dollars per address on the open market now, depending on the prefix that you buy.

That changes things. It changes the relationship between members and the registry, between different members in the community. And it sort of brings—the risk of these kinds of situations becomes a little bit more prominent. So we're definitely watching very closely.

Before I sign off, I should also—and I should have mentioned this in the presentation, the next RIPE meeting will actually be the 16th to the 20th of May. And we're hoping—knocking on word, crossing fingers—that it will be in Berlin as a return to physical meetings. And that will be followed the month after that by ICANN in The Hague. So there's going to be a lot going on in Europe, hopefully, around the middle of the year.

Yeah, thank you. I really enjoyed presenting this. And the questions were really interesting, too. Thank you very much.

SÉBASTIEN BACHOLLET: Thank you, Chris. I feel that MoU signed by Olivier and the CEO at that time of RIPE NCC was a good move, and now we have to put it at work. and I thinks this type of meeting is one way to do it. And I appreciate that you put the link to your training or eLearning site because it's something that could be very useful for our members too, and therefore it is great.

Okay, I will thank you, every participant, and once again, thank you, staff, for organizing and monitoring this meeting. Thank you for the interpreters in both languages, French, Spanish, Russian and English. And thank you very much, both Frederic and Chris. Well done. Talk to you soon and hopefully, in Berlin with Chris. Will be great. Thank you very much. Have a good evening. Take care. Bye.

MICHELLE DESMYTER: Thank you, everyone. Meeting adjourned.

[END OF TRANSCRIPTION]