ICANN72 | Virtual Annual General Meeting – GNSO: NCSG Membership Meeting
Thursday, October 28, 2021 – 10:30 to 12:00 PDT

MARYAM BAKOSHI: Hello, everyone, and welcome to the NCSG Membership Meeting. My name is Maryam Bakoshi, and I am the remote participation manager for this session.

Please note that this session is being recorded and follows the ICANN expected standards of behavior. During this session, questions or comments submitted in chat will only be read aloud if put in the proper form as noted in the chat. I will read questions and comments aloud during the time set by the chair of the session.

If you would like to ask your question or make your comment verbally, please raise your hand. When called upon, kindly unmute your microphone and take the floor. Please state your name for the record, and speak clearly and at a reasonable pace. Mute your microphone when you are done speaking.

This session includes automated real-time transcription. Please note this transcript is not official or authoritative. To view the real-time transcription, click on the closed caption button in the Zoom toolbar.

With that, I will hand over the floor to the chair of the NCSG. Bruna, please. Thank you.

BRUNA SANTOS: Thank you so much, Maryam. Hi, everyone, and welcome to the NCSG Membership, our open meeting at ICANN72. To those of you who don't know me, I am Bruna Santos. I am the chair of the NCSG currently. And I'm also joined here by some of our leadership, by some of our councilors and a few other members of the ICANN community.

Before we start this meeting, I just wanted to go through the agenda with you guys. Our agenda is quite quick and short for this time for this meeting. And we are going to start with a short demo from Theo from Realtime Register. It's about DNS abuse and a monitoring system.

Up next, we're going to go with the constituency updates, so I'm going to have Raoul and Raphael and Ben. Raphael and Ben are doing the leadership transition right now, so we're all going to talk and listen a little bit to what's going on in our constituencies.

Then we're also going to talk a little bit about council and policy committee updates. There are a lot of transitions going on up there as well, so I'm welcoming Tomslin.

And last but not least, we're going to just do a short discussion on membership engagement. I know this is something that has concerned many of us in the past months, and I just wanted to use this as an opportunity for us to start a new conversation about how are we engaging our members through this kind of hybrid moment that ICANN is going to have in the near future.

Last but not least, we're going to do AOB. This is also going to be an opportunity for Maryam to say hi and for us to thank her for her outstanding work in the past years and also welcome [Andrea].

So I'm not going to take any more time from this meeting. I'm going to hand the floor to Theo. And thank you so much, Theo, for your offer and for accepting our last-minute invitation. You have the floor now.

THEO GEURTS: Thank you. And it was indeed last minute. My name is Theo Geurts. I am at RiskReact. That is a cyber intelligence unit Realtime Register. Realtime Register is a Dutch registrar, and we do a lot of research when it comes to DNS abuse. And it's ICANN72, so another DNS abuse meeting is very appropriate. We don't have enough of those anyways. But I'm going to switch things up. I'm going to share my screen here. If that could be enabled for me, that would be really handy.

BRUNA SANTOS: Maryam, can you help us with the screen?

MARYAM BAKOSHI: Yes, we'll do that now. Thank you.

BRUNA SANTOS: Thank you so much.

THEO GEURTS: Thank you. Always disabled, participant screen sharing. So to get it working, I really need the share screen because we're going to do a live demo and we're actually going to look at actual malicious DNS abuse. We're not going to use any slides here, so now PowerPoint [like that] or anything. And, oh, here we go.

So let's first start with a basic question that I'm getting asked a lot: "Why on earth did you set up such a system?" Basically, we go back to 2018 when I was looking at what ICANN OCTO was doing with their DAAR program and I thought, "Hey, that would be really, really handy if we had such a system like that."

And when I came back home at the office, we started floating the idea like why don't we make a dashboard and roll all these reputation blocklists into one system and try to visualize DNS abuse. Then we got the idea like maybe it's also handy if our resellers also get their own dashboard so they can look at how much DNS abuse they have, where it is located, what is happening, etc. It was sort of a situational awareness idea that we got.

So we started working on that, and it took a lot of effort, first of all. There are many reputation blocklists out there. We started working with Pulsedive.com and Pulsedive.com is sort of an open threat intelligence platform which you can use for your investigations. One of the cool things was they have 30 reputation blocklists available. That made sense to implement Pulsedive first, then we already have 30 blocklists to deal with. They had data going back to 2018, so there was

a logical idea to use them first. We are now up to 75 blocklists, so we've grown quite a bit.

I'm aware that the dashboard is not very visible to people with a small screen. That is something we still need to work on. On the other hand, I have a zoom button, so let's zoom in when we need to.

Let's first zoom in on how much abuse does Realtime Register now actually have. It's good to know that we have a wholesale platform with resellers. We also have a backend registrar service, which means that there are also other ICANN registrars who use our platform. I mention this because we can benchmark against other registrars on our platform how they are performing the DNS abuse, and we can take a collective total sum of all the DNS abuse of all these other registrars on our platform.

Now we are not GoDaddy. We've currently somewhere around 3.1 million domain names on the platform, so we don't represent the entire DNS. But given the fact that we have many thousands of resellers, I think it's a good reflection of a large part of the DNS. Still, there's some systemic DNS abuse going on with a few registrars which is causing a lot of problems. But here we have 0.03%, and that is very, very low.

And if we look at a breakdown of how that looks like, it looks like this. I will make the screen a little bit bigger. Since 2018, we have discovered 546 domain names which were malicious. These had 2,000 indicators. And indicators you can replace with the word URL. So there were 2,000 URLs, 411 are still online, and 135 are offline. We get back to that a little

bit more why there are only 135 domain names offline because that is pretty significant when you look at the policymaking point of view.

And apologies that some stuff is in Dutch. I'm using a Dutch version of Windows, so there's Dutch language settings all over the place.

So we can look at this system how many abuse there is per TLD. If we look at the current chart, we can see a little bit more where that is clustered, how much that is, and we have around 300 .coms. We mark that as green because when you have a total of 3.1 million domain names and we have a lot of .coms also, there's more than 300 .coms listed as abusive, we still mark it as green because it's still low.

If you look at the other side of the spectrum, we've got .pw. We mark that as orange because we only have a few of those. And if you only have a few and a few of them are malicious, then it gets marked into the red zone. We've got .nl. We've got .online. Most of the European ccTLDs are ranked very, very low, and it has [definitely to do that] most ccTLD registries are pretty keen on combatting abuse so that is pretty low.

And you have to wonder if you talk about the NIS2 directive, if such a directive would be actually useful because the abuse levels really are actually very low. And we can see from this chart that the abuse levels are happening on different levels, in a different country actually.

So we go back to the report. When we are talking about that there are only 135 domain names offline, that has to do with a couple of things, and that is currently where does DNS abuse reside. And this is quite…actually, back then it was a shocker for me because I was

expecting when we would load up all these reputation blocklists that we would have a lot of domain names being marked as malicious. And basically, that did not happen.

It was very, very low. And when we look at the distribution of the malicious domain names, 82% is happening on a URL level, 16% is happening on the domain name. That is something that as a registrar something that most of the time [can] take action on. And then we have 2% that is happening on the hostname level. Now the URL level and the hostname level, that is something that is out of technical reach for a registrar. That is happening at a hosting level.

Realtime Register does not provide any email services, hosting services, nameserver settings, etc. We don't have that. We only do domain names. So when you look at 82% happening on a URL level, that is for me as a policymaker within ICANN and as a registrar who has actually to do something regarding domain name abuse, that is significant. That is one of the reasons that we made these reports available to our resellers so that our resellers can take action. We also send them notifications every time, every hour that we find new domain names, we inform the reseller like, hey, this is happening.

But it's very important to understand that a lot of the DNS abuse is happening on a URL level, and that is outside of the contracts which we have with ICANN. So if you want to talk DNS abuse and how to combat it, it's very important to understand that the majority is happening on the URL level.

So when we look at all these domain names, these are all domain names that have been marked for malicious activities. It could be phishing, it could be malware, it could be BEC fraud though that is not very visible nowadays. But it's a whole list of domain names, and we are going to actually look at one of the domain names right now.

We're going to zoom in. What we have here is a typical case of malware distribution. As you can see, it is happening on a domain name techcouchits.com. I hope I pronounced that right. But as you can see, a lot of this is not happening on a domain name level itself. It is happening on a URL. Again, for us as policymakers within ICANN, that is an important distinction. Again, they are outside of the contracts, and we need actually somebody at a hosting company to take care of these URLs which are apparently there's malware there.

URLhaus is one of the feed providers. They are operating from Switzerland. They are, in my opinion, an excellent feed. If we talk about trusted notifiers within the ICANN silo, for me URLhaus is a very respectable reputation blocklist provider. Most of the times, these people have it right. So that is important to know when we are talking about DNS abuse.

We can take a couple of other feeds here. We can go to webnode.es. What we see here is a lot more going on. There's a whole lot of stuff going on. I see some back phishing and I see some credential phishing for social media.

What is good to know is when you look at the registration date of this domain name, it's registered in 2008. What we see lately is a shift when

it comes to domain name abuse. In the past, we would see quite a majority of malicious domain name registrations and these domain names would get active within a couple of hours or a couple of days. And those domain name registrations were obviously malicious.

But what you have here is a domain that has been registered in 2008. The registrant is a legit company. So when we talk about verification or validation as a countermeasure to combat DNS abuse and you have a shift and it's happening a lot on the URL level, you lose a lot of investigative evidence. Because what we see now is these URLs are usually always hacked and [inaudible] that these websites are being hacked.

And if websites are being hacked, that is significant in the policymaking because we always understand that in DNS there's a nice hierarchy. It's nicely structured. We've always got the registry on top, and then we've got the registrar below it, and then we have the reseller, and then we have the hosting company.

For people who are not well versed in DNS, people sometimes make the assumption why not start regulating at the top there at the registrar level and every regulation or contractual requirement will flow down nicely through the entire DNS. That is not what is happening because when we look at URL abuse, hacked websites that is happening outside the technical realm of the registrar.

But it also means that if you look at verification and validation of the registrant, a hacked website will not provide you, for an investigator, with relevant information. We don't have a domain name registered by

a criminal. No, you have a domain name registered by a legit person. You don't have a money trail because no domain name was registered. The website was hacked, so you don't have the money trail.

And you don't have an email address that you can use for a reverse WHOIS operation to see if there are more malicious domain names. Basically, the only thing you might have is in some server log that there was an incident and you might have an IP address, probably behind a lot of proxies bouncing off all over the world.

So as an investigator, you do not have a lot to go on. You can maybe find something in the payloads of the website where there's the malware. You might do some malware analysis, and you might be able to find some clues there. But basically, that is it. And that explains why a lot of phishing, malware operations go undetected and go unpunished. And it's becoming a really real problem. I mean, every day we hear about a company being ransomwared, etc.

Now for us having access to all this data also means we have a commercial edge, if you will. When we talk with registries about doing a promotion, for example, a lot of registries offer that but a lot of registries don't want to have abuse because abuse is basically costing them money. It's costing us money because we need to clean it up, we need to do something about it.

So registries, for example, like the Dutch registry .nl or you have .org, they have something like a QPI program. Such a QPI program will get measured on several quality performance indexes. So they measure abuse. They measure your renewal rates. They measure stuff like is the

domain name being used, is there an email address, etc. The more performance indicators that you hit, the higher the discount. So abusive domain names might lower your discount, and we are operating in a pennies game. If we get only 10% from a pre-dollar discount, that is for us massive if we get penalized for having abusive domain names. Being able to monitor that all is for us relevant.

I'm aware that this chart does not show you a whole lot here because this has been redacted, but normally what we can see here are the resellers being displayed here so we know exactly which reseller is causing abuse. And in combination with the other chart, the abuse per each TLD, we can combine such information and we know exactly we have a reseller here. The promo that he is offering to his customers is being used by criminals, and we are now not going to meet our targets with the registry. We are not going to get the full amount of discount. That is going to be a problem, and then we will take active measures.

I can't tell you what the active measures are actually, because we've never been in that situation so we haven't created the procedures yet. But from my point of view, we still keep growing. We still keep getting more customers. So at some point, we will have a reseller with lax fraud controls on their side, and there will be criminals who will be abusing that reseller. So that's good information for us to have such monitoring all the time.

We can look at the abuse types which are there. I won't go into it too much, but the majority is phishing. Then there's quite a lot of malware going on. And then there's some spam and other types of abuse. So we

have that information at the fingertips, and we can also see which feeds we get the most information from. And in this case, we got a lot of information from Google, from their Safe Browsing API. More than 53% is actually coming from Google.

It's also good to mention if a domain name is mentioned on the Google Safe Browsing reputation blocklist, that also ensures that people no longer can visit the website without getting a huge warning. So be mindful of that.

I'm cutting the demonstration a little bit short to see if there any questions at the moment.

BRUNA SANTOS: We have, Theo, I guess we have Tomslin and Farell with their hands up. But Stephanie has also asked you some questions, Samaneh as well, in the chat with regards to…I lost the questions. But where does the data come from, if it's either from blocklists or Realtime Register's own clients? Stephanie also had some questions with regard to who are you responding to, who are the websites responding to as well in terms of the requests.

THEO GEURTS: Oh, that's a whole lot of questions. I suggest we start with the people who have their hands up, and then I will try to recap some of the questions you just mentioned. How's that?

BRUNA SANTOS: Great. Great, great. Then we can go with Tomslin, then Farell, and then Samaneh.

TOMSLIN SAMME-NLAR: Thanks, Bruna. And thank you very much, Theo, for this. I've actually never seen one before, so it's quite interesting to see. I just wanted to go back to when you showed us the various DNS abuse attacks. I missed…the pie chart didn't have which one had what percentage, and I was wondering whether we could see that again to know which of the abuses took the different portions on that pie chart if it's possible.

THEO GEURTS: You were referring to this one. Oh, no. No, this is the wrong one, actually. So here we go. That's the one.

TOMSLIN SAMME-NLAR: Yes.

THEO GEURTS: This is where we define the phishing, the malware, the spam, and then somewhat of the general abuse. You know, general, we've got to rely a little bit on the metadata from the RBL. Like when I go into an RBL like this, this is only what we get from some of these RBL providers. We only get a URL. We maybe get a risk or how high that is. We maybe get a category of it's malware. But sometimes these things are all missing, so we have to sort of compress that to a general abuse because we don't have the specific information. And then you get a pie chart like this

where 60% could be anything. It could be BEC fraud, it could be a romance scam. I'm just making something up here. It could be a lot. So for us it's important to know that phishing and malware are the biggest contributors to DNS abuse. Do you have a further question about that?

TOMSLIN SAMME-NLAR: No So the orange is phishing?

THEO GEURTS: Yes.

TOMSLIN SAMME-NLAR: Okay, cool. Thanks.

THEO GEURTS: And then we can go to Farell, I guess.

FARELL FOLLY: Yes, thank you very much for the presentation. I think one of my questions has also been voiced in the chat. Is the source of the data…as far as I can see, this is more or less a reporting tool. So where does the data come from? Are the registrars reporting the DNS abuse to you? Are the users? Or do you have some contracts with a bunch of server or Internet service providers that do that for you? Or if my email account got a spam, does Google report that to you? And how exhaustive is that data collection step? That was my question, actually. Thanks.

THEO GEURTS: That's a good question. The answer is twofold here. Let's focus first on the reputation blocklists. You've got parties like Netcraft, Google. Spamhaus is a very known one. You've got SURBL. So you've got a lot of parties like OpenPhish, PhishTank, Phishstats who report on phishing for obvious reasons. And they make the data all available. They have various lists which you can download or you can connect to your API. For that matter, Pulsedive is a paid version for that.

So we connect to all these APIs and we download all these lists. And some lists we download every day, every 24 hours. URLhaus which is also for free which is an excellent list, as I said, we can query that every five minutes [off the top of my head]. So we ingest all that data into our system, and then we go to match all that information. And if we get a hit, then it shows up in the dashboard. And if we get a hit, we send out a notification to our resellers like, "Hey, URLhaus found this URL. It's classified as malicious. Please investigate it and take it down if it's required."

So that is basically the bulk of the information that we have. The other sources are what we call cyber intelligence monitoring. That doesn't have a fancy dashboard. We don't share that with our resellers directly. It's processes a lot of data from email providers, security operations centers, but also organizations like the NSA, CISA, FBI, security research companies like CrowdStrike, FireEye, etc., security researchers. Most of the data is related to cyberterrorism, cyber mercenaries, huge attacks which are happening every day.

And that gives us information there might be domain names from our resellers involved in these major attacks. Let's check it out and if we need to take action, move forward with our resellers. But those reports are highly technical, so there are two tracks here.

FARELL FOLLY: Thank you very much.

THEO GEURTS: Excellent. I lost track of the queue. It's either Stephanie or Tomslin.

BRUNA SANTOS: I think it was Samaneh and then Stephanie.

THEO GEURTS: There we go.

SAMANEH TAJALIZADEHKHOOB: Hi, everybody. Hi to you all. I am the DAAR project lead, actually also joining from the Netherlands. I'm very glad to see the project that started, the idea of this project which looks very promising, I have to say. I have a couple of questions about some details of the data. For instance, I was wondering whether the data that goes in as an input, is it only the blacklist on your own customer base or you look at the domain space in general?

THEO GEURTS: Okay, that's a good question. No, actually, can you clarify it a little bit?

SAMANEH TAJALIZADEHKHOOB: Sure. I mean, I think somewhere in the demo I saw that you are comparing the amount of security threat domains you see on [inaudible] blacklist to the size of the TLD. I was wondering by size do you mean the size from the perspective of your registry or registrar, or is it the general size as in like [you have the] zone files?

THEO GEURTS: Okay, so the information that you saw in the demo, that is basically based on the information of the domain names registered on our platform, so not the zone file.

SAMANEH TAJALIZADEHKHOOB: Okay.

THEO GEURTS: But since we have information from the reputation blocklists—and you might know this, others may not—but the reputation blocklists contain information about all the registrars, the malicious domain names, and all the registries. And we also have access to the zone file, so we do a little bit of probing that to see how our competitors are doing. But we don't do that in depth because it's actually a lot of work. So what you see in the demo is through our registrations on our platform and we do some probing on a larger scale.

SAMANEH TAJALIZADEHKHOOB: Okay, I understand that. I can imagine that that probing is probably more accurate for gTLDs and less accurate for ccTLDs as their zones are less public, so less access to the sizes where they are not registered with you.

THEO GEURTS: That is 100% correct.

SAMANEH TAJALIZADEHKHOOB: Okay, great. Another thing that I [doubting] also because we are dealing with it at the moment at OCTO is how do you choose an RBL as an input. As somebody who is in this field for a long time, I know most of the few that you are using. And I can imagine that because you work with the data you gain lots of experience about the accuracy yourself. But is there any method that you use to choose, or it's just based on your own knowledge?

THEO GEURTS: Yeah, it was actually based on experience. I mean, in 2018 we started to look at these reputation blocklists. Except from hearing about them I never looked into them, so that was quite interesting to look at them. Yeah, let's give it a short answer. When I look at experience, and most of the experienced that I've gained when it comes to blocklists is when I was a volunteer at the Cyber Threat Coalition [inaudible]. We set up as volunteers our own blocklist there, and that gave me actually a behind-

the-scenes insight on how you actually set up a blocklist. What is involved, which metrics do you use? So when I look for new blocklists, I look at how is this blocklist set up. And I start investigating how good it is, where do they derive their information from. So you take a lot of metrics in my mind based on experience like this is what I want. And of course, it also needs to—and this is an important metric for me always—I need to have a lot of hits.

SAMANEH TAJALIZADEHKHOOB: Yes.

THEO GEURTS: That is basically a guiding principle. I mean, if I only get one or two hits on 3 million domain names, that is not worth my time to implement that one because that is just too much expense for a developer to actually set up an API, implement an API for only two domain names.

SAMANEH TAJALIZADEHKHOOB: Mm-hmm. Yeah, I understand that. That's very clear. I think for the sake of time of the discussion, I have a lot more questions, but we can discuss it offline with you. We are at the moment working on a methodology for evaluation of RBLs with certain limited metrics, so maybe it's also useful for you guys and for your work.

THEO GEURTS: We can reach out.

BRUNA SANTOS: Excellent. So I think up next is Stephanie.

STEPHANIE PERRIN: Thanks very much, Bruna. Thank you, Theo. This is fascinating. I wonder, we are being called upon to define abuse. And I understand why from a registrar's perspective you would want just a broad term like abuse. But from a criminal investigation perspective—and I must say my question is informed by the fact that I'm quite alarmed at the attempts to curtail hate speech and have domains taken down by any number of actors if they offend people—so there's all kinds of crime in these RBLs.

But there's also what I would call confidence scams. For instance, romance scams. Not strictly speaking illegal. Even the grandmother and grandfather bail me out of jail scams are strictly speaking hard to prosecute. Because if you're stupid enough to not know the sound of your grandson's voice and send money off into the wild blue yonder, it's tough prosecuting that, right?

On the other hand, there's malware that's being imbedded if I'm dumb enough to click on a "your domain is going to expire if you don't contact us below, click," that kind of thing.

So how the heck do you define this? And then the next question: Is there any regulation at all of these RBLs? Because the potential for state mischief in terms of blocking competing countries' domain names "by accident" or otherwise is enormous. And if there's no regulation and no

international agreements, what is stopping that from happening? Thanks.

THEO GEURTS: There's a lot to unpack there, actually. But let me see if I can….

STEPHANIE PERRIN: Sorry about that. How about the definition first, and then the state mischief?

THEO GEURTS: See, when it comes to the blocklists, you are in control of what you want to ingest. There are blocklists that tell you what porn site is. So you have these blocklists. Now we don't have any laws around porn. And personally, there are maybe resellers in India that might be affected by such laws and regulations. But for me as a registrar, I'm not going to use those blocklists.

There are, of course, blocklists around hate speech, [oppressional] speech, or whatever speech. I'm not going to render any judgment there, so I'm not going to use such a blocklist.

I'm only looking at blocklists that give me information about malware, phishing, and that kind of stuff which is [sort of] what we have defined within the DNS abuse framework. I'm pretty sure your familiar with that one. We specified a couple of definitions there, what is in scope of a registrar. That is sort of my guiding beacon there.

I mean, CISA, there's no blocklist there actually that you can use for CISA. But that is stuff that we take down. And that is how you—at least me—that is how I base my decisions. This is a blocklist that we can use. This is something that is completely content related and that is outside of my scope for this reason. So you are actually the master of your own house there. You are in control.

Then you get to the question—and I find this a really cool example—this is a blocklist that is called CoinBlocker Domains. CoinBlocker Domains, there is no law against coinblocker domain names. What happens when you visit a coinblocker domain name, at that moment you are visiting a domain name and the domain name or the website in this case will start to mine for cryptocurrency using your computer. It's using your computer time to mine that cryptocurrency. Now there are apparently people there that are not happy with such practices. It's not illegal, and this is where we said, okay, this might be a blocklist that is good to know for our resellers that it's happening. So we are providing that blocklist to our resellers. What our resellers do with that information, that is completely up to them.

It's a little bit the same in my opinion, we also [parse] a blocklist from the Global Cyber Alliance. They have a blocklist there that deals with scam domain names. I think the blocklist is Scamadvisor.com. When we first loaded that blocklist, it showed about 400 domain names. When I looked at it, I thought are these really scam domain names? I don't know.

But it's maybe interesting that our resellers can inform their customers that it's on a blocklist. We don't know if it's actually a scam. We don't know if it's actually malicious. Because if something is malicious you are supposed to, of course, investigate it. But something like a scam domain name, then you get into a territory of is it really a scam or is it not? Now some scams are really easy to detect and some scams are really, really hard to detect. Some are false positives, and you are dealing with a real e-commerce website web shop.

But that it is on the blocklist itself or on a blocklist, that information should trigger you to look into it. Because if you are on a blocklist for the right or the wrong reasons, if it's for the wrong reasons because it's a false positive, you need to look at it and see if you can get yourself removed as a domain name holder because it will affect you on many, many levels.

And if your domain name is listed on Spamhaus, you're going to have a lot of problems receiving and sending email. So if you are on that list by mistake or for whatever reasons that I don't know, I think it's good information for our resellers that they are aware that some domain name is listed on a blocklist for whatever that reason is. And it's up to them to take action. Does that answer it?

STEPHANIE PERRIN: Yes, that's a big help. It does raise another question. As you say, registrars are operating for pennies in this game. I've heard an awful lot at ICANN about how we desperately need to see personal information so that we can fight crime. I'd like to know where the hell the money is.

Why would anybody—for instance, it's far easier for you to just block a domain or yank it down than to actually spend time investigating it, right? I've heard from plenty of other people saying they've seen the same bad guys up there 10 years after they were first spotted. It's not worth anybody's while to take them down. To be fair, it's not their jobs either. And we all know how difficult a cross-border investigation is. So where's the money? There's got to be some money in here, or people aren't going to fix the problem, right?

THEO GEURTS: Are you asking me as a registrar or more from a security company point of view?

STEPHANIE PERRIN: Either one.

THEO GEURTS: Well, of course, a lot of these…there are RBLs providers that, of course, do a lot of research. Their blocklists are pretty good, and they charge you a fee to use it if you want to have that information. And let's be fair. Out there, yes, there are lots of companies that rely heavily on companies like Spamhaus or Netcraft. I mean, they use their blocklists to protect their networks. It makes a lot of sense to me to use that information. It also makes lots of sense to me that these companies get paid, so there's the money for them.

As a registrar I think the question is…okay, let me put it a different way. What we have at Realtime Register is a sort of [pre-crime] algorithm. We call it Samaritan. What we do is based on certain metrics our abuse team gets a list of domain names that are being flagged by the program. Since it's an algorithm though, we've got to be careful with that. And that algorithm provides us daily with a couple of domain names that need investigation. And when you go down that investigation, it's going to cost you money. But a lot of times we can take down domain names before they become malicious. That saves us a lot of time because we don't get a report anymore, so there's a little bit of saving there.

It has another side effect. When we look BEC fraud, we had that happen in 2018. We were proactive. We took some stuff down before it even went online because we had 100% confidence that we were dealing with the same criminals again over and over. What happens is these guys move on and they go to a different registrar. That was a sad reality, but for me as a registrar I'm saving a lot of money there because I don't get the reports. I don't have to investigate it. I don't have any reputation damage there. So there's money saved there.

And basically this system is also automated, so a lot of the reports go automatically to the right source where they can deal with it. So that saves me a lot of money also because I don't have to email 100 times a day. That's an exaggeration. Like 10 times a day. So that saves money.

STEPHANIE PERRIN: Thanks. That's a great answer. As I suggested in the chat, I think we have a whole pile of more questions for you but no more time. So maybe we

could invite you back, and I'll volunteer to pull together the questions from the chat transcript and any others and we can pick your brains again.

THEO GEURTS: Sure. Happy to. And there's lots more to discuss. I mean, this was just a very high-level, very quick overview due to time. There's lots more to discuss. I'm happy to do it, so reach out. Thanks.

STEPHANIE PERRIN: Thank you very much. Very useful.

BRUNA SANTOS: Thank you so much, Theo. I guess, as Stephanie suggested, we can definitely do that. I think Andrea has already copied some of the questions we had for you, so I might send you an email in the upcoming days just so we can see when is a nice date for us to invite you to one of our meetings if you're agreeing with that. So thank you very much for the exchange again.

THEO GEURTS: Sure. And enjoy the rest of the meeting.

BRUNA SANTOS: Thanks. So, guys, let me open my camera again. I'm so sorry. Yeah, just for us to move on with our agenda because this is a shorter meeting, we have until the top of the hour. So depending on where I am we have

until 9:00. So I want to follow up with the second agenda item which is constituency updates. I have invited both Raoul and Raphael and Ben to provide some updates on NCUC and NPOC. I don't know who wants to take the lead on that, but I see Raphael with his camera on. And now Raoul. So whoever of you that wants to come in first, I'm handing you the floor.

RAPHAEL BEAUREGARD-LACROIX: Should I go first? Is that fine?

RAOUL PLOMMER: Go ahead.

RAPHAEL BEAUREGARD-LACROIX: All right, thanks. Hi, everyone. Raphael here, chair of the NCUC EC but not for long still. Yes, so a few things today, one of them being the leadership transition but I'll finish with that. But otherwise, two small points.

The first thing is just kind of an update a little bit of what we've been doing at the EC and, let's say, a project that we set up in a way is a targeted outreach—or we should say in-reach actually—to organizations which are members of NCUC. And so this was done by region, given that the EC is also divided by region already, the EC seats, and so we thought it would be a good idea to proceed that way.

And so basically what we're doing is we made a list of each of the organizations that are members in the different regions and we reached

out to them and asked them…some of them, some organizations probably members of NCUC for a very long time, maybe at the time where there were people who were interested in DNS policy in that organization. It might not be the case anymore, but for some it might still be the case. We have big organizations, small organizations, known ones and less known ones. But we thought it would be a good idea to reach out to all of them and ask them basically if they are, in a way, still into DNS policy and what we can do for them or what they can do for us as well. So just reinitiate a dialogue with some of our organizational members.

So we set that up over the summer. We started sending emails in the fall now. I don't think we have got a lot of answers yet, but we are hopeful that maybe with a little bit more prodding we'll be able to get something out of that. And the point, of course, would be eventually if we have organizations that are interested or that still want to participate in DNS policy in the non-commercial sphere or environment, that we would get them on board for some form of event or meeting or something depending on what they're up to.

Yes, so that's one of the main things that we've been busy with at the EC. The other part of my very short speech now is also to remind everyone that we still are looking for someone for the Asia Pacific seat on the EC. We do not have anyone for the election. And so if we have anyone currently listening who is a member from the Asia Pacific region, please reach out to other people that you know or put yourself out as well.

You can just write to chair@ncuc.org. You can write to me personally. You can also write to Benjamin who is going to be taking over as chair at the end of this meeting, chair of NCUC, or any of the EC members actually. That would reach us in any case. Yes, and if you know someone or if you yourself are interested, please step forward.

Of course, I don't want to say that it doesn't require a lot of work because we are looking forward to EC members who will be able to put some time and be engaged. But at the same time, it is a leadership position but it's not one that comparatively requires a very heavy time commitment. Although it does require some work and some engagement, of course, and some time on your part. So, yes, but it's very fun and you will have Benjamin along with other experienced members of the EC along with you. So, yes, we're still looking for someone for that.

And the third point finally is the leadership transition. So as I already announced, in the last election cycle I was not stepping up for election. Benjamin was elected, and now is the time for leadership transition. So I would like to take this opportunity to thank everyone in the community, of course. Thank you for your engagement over the year and thank you also for participating in the meeting that organized in the spring as well, which I think was successful.

And I will remain a member and I will still be active and participate, but as I explained previously my other time commitments do not allow me to put in all the time that's required for a position such as chair of the constituency and so hence, I step down. I will still be there to support

Benjamin during the transition and also [inaudible] needs to. And I will remain, yes, as I said, a member of the NCUC and NCSG.

And also I would like to thank [some persons] [inaudible], but this was already announced on the mailing list before, but thank Maryam for her support during all those years and during the time that I was in leadership position as well. And looking forward to working with Andrea, although I will not be directly working with you anymore as I won't be holding any leadership positions for the time being. But, yes, welcome Andrea as well.

So that is all for me. And I guess if anyone has maybe specific questions about something, anything that I mentioned just now. Also, Ben, if you would like to, you can also take the floor. I don't know if you have planned anything. If you wish, that's a possibility too.

BRUNA SANTOS: Thank you so much, Raphael. I don't know if Ben was going to open his mic. Were you, Ben? I don't think so.

RAPHAEL BEAUREGARD-LACROIX: That's fine.

BRUNA SANTOS: I'll also take the opportunity to thank you, Raphael, for your work and dedication to NCUC in the past year and a half. So thank you so much. It was a pleasure to work with you. It's a lot of like…it's a meeting of transitions. We have a lot of people coming, changing places and areas.

So it feels kind of bittersweet to see some of our people go, but I do hope you all continue to be engaged with us and actually doing the good work for NCUC, NPOC, and NCSG as well. So thank you also, Raphael, for all the work and the support as well.

RAPHAEL BEAUREGARD-LACROIX: Thank you.

BRUNA SANTOS: I'm going to hand the floor to Raoul now who I expect doesn't likely know about anyone that's leaving the NPOC. But, Raoul, you have the floor.

RAOUL PLOMMER: Thanks, Bruna. Well, I'm going to keep it short and sweet. So basically, I guess, the biggest news that happened since last ICANN meeting with NPOC was that we finally finished our charter work. And that's including the annex which makes it easier to modify things that aren't as crucial or don't need to be hard coded into the charter. So they can be changed just by the EC and not go through the whole ICANN process of modifying a charter. I think does actually NCUC and NCSG have such a thing? An annex?

RAPHAEL BEAUREGARD-LACROIX: I'm not sure. I'm not quite sure what you mean by an annex.

RAOUL PLOMMER: Yeah, like something that is not quite as high-level as charter but something….

RAPHAEL BEAUREGARD-LACROIX: We have operating procedures. Maybe that's what you are [inaudible].

RAOUL PLOMMER: Yeah, that's pretty much it. So, yeah, there's that. We also had some ambitions of creating a bank account for an international group such as ourselves, but apparently it's not possible even in Estonia. I had this confirmed by an Estonian friend who asked one of the banks. I mean, I guess I could pursue this and go to other banks, but I think their requirements will be very similar. But I think we are still pursuing creating an NGO platform in a way that we would want to register NPOC as an NGO. That would allow us to do some things that we can't as an unregistered organization as we are in ICANN.

We've done some work as well, ICANN work, in the IGO working group. Unfortunately, I cannot tell you much more about that. It was handled by Ioana and I think Caleb.

We also went through or have been going through this NomCom review working group that has been going on since Panama. That makes it three years now. It looks like they managed to kick down the can one more time. And now basically what I grasped of that whole process was that basically at least the single most important item for I think both NCSG and especially NPOC was that we still don't have a seat that

actually any sort of objective outsider would say that we would really deserve that. That's been also pointed out by the Ombudsman as a fairness issue, lacking it.

Yeah, I think that's pretty much it. If you have any questions, please let me know.

BRUNA SANTOS: Thank you so much, Raoul. I think there is one question from Stephanie in the chat with regard to the charter: if it's been approved so far and where and whether it's published yet.

RAOUL PLOMMER: No. We actually finished it last week. So no and no.

BRUNA SANTOS: Great.

RAOUL PLOMMER: But it's already been sent back to the ICANN Org, and I think the lawyers are having one more look at it just to see there's not anything too dodgy in there.

BRUNA SANTOS: Great. So we should see this in the coming weeks, right? Hopefully.

RAOUL PLOMMER: Yes. Well, never say never, but….

BRUNA SANTOS: And congrats to NPOC for the work as well. We do hope to see it published and public as soon as possible. I don't know if anyone else has any other questions for NPOC or NCUC in this exchange.

I know that one good work that you both have been focused on were the recommendations from ATRT3 and also a lot of the things that were suggested in terms both to our stakeholder group but also to our constituencies. I know this is an ongoing kind of work, but maybe it's something we can also discuss in a few weeks' time or in a future BC meeting when we had all time to take in the suggestions and improvements suggestions to be [accepted] and then present them to the community as well.

So if you don't have any more questions for our constituency chairs, I'm going to move on to Agenda Item #3 with Tomslin. Tomslin is also somebody else who is transitioning, so we also have a few changes on the BC. Also, we have a few changes on our representation at the GNSO Council vice chair position. So, Tomslin, I will hand you the floor and let you explain to everyone what's going on.

TOMSLIN SAMME-NLAR: Thank you, Bruna. All right, so regarding the transition bit, we do have a new councilor, and that's Manju. Tatiana has now left us from the BC. And I have been appointed the vice chair for the non-contracted parties house of the council. So that's pretty much it about transitions, I believe.

But let's talk about some things that happened in the last meeting since we're having this meeting after the council meeting. I think there are only two things of interest. One is that the EPDP Phase 2A final report was adopted. I think, Stephanie, that brings your work to an end, and Milton there.

The other one was we had a motion to update the GNSO councilor job. The NomCom appointment is for a GNSO councilor job, and there were some proposed changes there for NomCom to prefer candidates which are not currently affiliated with an SO/AC or any GNSO stakeholder group. That didn't go forward. That motion was deferred for further discussion, so we'll revisit that in the next meeting.

The other thing that came up was that a couple of, many stakeholder groups and Cs have concerns regarding the fact that policies that have been approved by the GNSO Council are taking too long to be considered by the Board or implemented. So I just wanted to ask our a community a question whether we have such concerns at all. Yeah, basically that.

And then the other question I have for our community, again, is the thought paper which I forwarded to the mailing list two days ago from Org on [more] defined consensus policies. I'm interested to hear what members think about that once they read it.

And finally, we have some two vacancies which I'll be sending emails on the list about. I just want members to start thinking about it. The first one is one representative on the EPDP IRT. Stephanie has resigned from

that position, so we have that open. We'll be seeking for a replacement for her on there.

And a representative too to the council committee for overseeing and implementing continuous improvement—always a mouthful, that one—which is currently tasked to review the GNSO's statement of interest requirements. So we need a representative to that. I understand with that one there is not much work, so if someone wants something light, please get interested.

Thank you, Bruna. That is all I had.

BRUNA SANTOS: Thank you so much, Tomslin. I don't know if anyone that's on this call has any questions for Tomslin regarding the BC or any of the topics he just mentioned. I did want to stress this need for us to have more volunteers in some of these slots that Tomslin just mentioned. I do think that we can work on something that's more collective. That being you guys having meetings with somebody that's more well-versed or even understands more the topic of the specific working group or working party or group.

So if you're really willing to do so, it's a good opportunity to get to know ICANN, get to understanding [inaudible] our positions. And it will be an interesting thing to do, at least in my opinion. So let us know if you have interest in any of them, if you want to help. And that's it.

I see, Tomslin, Milton asked us if you could update us on the status of the EPDP vote in council as well.

TOMSLIN SAMME-NLAR: So that's on the EPDP, yes. I was trying to get the exact percentages. So like I mentioned, it was adopted and it was passed. The non-contracted parties house had 100% vote for this. Sorry, the contracted parties house had 100%. The non-contracted parties house had 61.54%, I believe. Yes, that is the summary of the vote for the EPDP, Milton. I don't know whether you wanted much more detail on that.

BRUNA SANTOS: I see Milton raised his hand up, so probably.

TOMSLIN SAMME-NLAR: Yeah, go please.

MILTON MUELLER: Sure. Hello. No, I just heard people coming out of that council meeting saying, "What the heck is going on? What did they do? Why are these people complaining?" It almost sounded like it didn't pass. I got a request from a journalist saying, "What is the status of this? It sounds like everybody is against it." So the final report was passed, is that correct?

TOMSLIN SAMME-NLAR: That is correct.

MILTON MUELLER: Okay. And as Stephanie said, now some of the work has moved into the IRT? And the accuracy, what is the status of this accuracy procedure?

TOMSLIN SAMME-NLAR: I'll let Stephanie answer that one because she is the rep there.

STEPHANIE PERRIN: Yes. Hi. Yeah, Manju and I are on the accuracy committee. It is chaired by Mike Palage. It is represented vigorously by a number of parties who were not particularly happy with the outcome of the EPDP policy. As you know, the accuracy program has been rather separate to policy. Of course, it would be because we didn't actually have a registrant data policy prior to this. But don't get me going down that rabbit hole.

So this is the scoping committee that we are on at the moment. And then, of course, that will flow into the actual PDP. Or at least one presumes that several of the people on the scoping committee will continue on into the PDP. That's the commitment that I'm prepared to make because this stuff is pretty arcane, as you know.

Now you probably saw a lot of reaction among our registrar and registry colleagues. First of all, and it's worthwhile checking the council transcripts because Kurt Pritz had a fairly lengthy intervention that confused many of us—myself included—that may have not been keeping up with the emails. But he had some complaints about the procedure and the arguments about whether particular recommendations were in scope or not in scope. And I invite you to have a look at that.

Yes, Palage, I'm just checking the chat as I go by. So Palage has us on a forced march on that accuracy committee. We are due to continue the work by August, and then excellent Barry Cobb came and presented on the details of the work and basically said you're not going to get it done by August and it's better not to be asking the GNSO for more time after. It's better to—I'm paraphrasing this, of course, Barry can put this in project planning language—better to under-promise and overdeliver.

Nevertheless, Mike made the decision to continue on an August timeline, which I'm not very happy about. Not that we don't want to get the work done, but if this means two meetings a week, you know how awful that gets. And it will mean two meetings a week because we can't agree on anything. And the vagueness that surrounds this entire accuracy endeavor means we're going to be fighting over mindless things.

There's a particular schism in here that will emerge shortly. And sorry, as you can tell I could go on for hours here, so just tell me to shut up. As you usually do, Milton.

MILTON MUELLER: Yeah, Stephanie, I didn't want to tell you to shut up, but I wanted to ask: the accuracy proceeding is considered a distinct phase of the old EPDP, or is it a completely new proceeding? And if it's a new proceeding…or if it's part of the old one, I thought that we had agreed that it was out of scope for the EPDP.

STEPHANIE PERRIN: Yeah, it's completely different. But that doesn't…I'm being ironic when I am saying that the unsolved issues of EPDP in the minds of some of our brethren are going to land in accuracy. This is just where the [bottle] has reemerged. Because this is a whole separate process and not necessarily linked to SSAD.

Now if I may comment on Tomslin's question about how we feel about things being slowed down at the Board. And bear in mind that council voted to accept the EPDP report, but the Board will ponder this. And the IRT that is dealing with both the previous phase plus the IRT for PPSAI, both need serious revision because they've been stalled. Without even discussing the transfer policy.

So there's a lot of…and you know that giant, master ugly sheet that Barry controls with the implications of the EPDP on other policy things, accuracy is one of them because we've never had an accuracy policy. We've only had accuracy requirements. And the other ones I mentioned. So our chances of getting this done in a year, I think, are slim. Because of course, yours truly, I hate to sound like I'm trying to be obstreperous but we will not be running roughshod over the policy that we spent so long hammering out in the EPDP and demanding the kind of authentication and accuracy that many people are looking for. And, yes, they are looking for authentication or registrant data.

So what can I say? I hope that answers your question.

In terms of what Alan Woods commented the other day, some of our registrar pals were quite upset that the objections to the EPDP in the vote were basically policy objections, which is not the role of the GNSO

members. That's a bureaucratic function in council. It is not an opportunity to dig in about the shortcomings of the policy. They've had their chance in their dissident reports. So that's what they were complaining about. I felt it was an abuse of the GNSO process. Hope that answers your question. Thanks.

MILTON MUELLER: Yeah, it wouldn't be the first time the GNSO process was abused. I'm still curious about the famous SSAD. Can you update me on whether that's happening or not?

STEPHANIE PERRIN: In the minds of many it's happening, but that is in the very obscure ODP phase right now. The Board is busy studying the ODP or developing the ODP, and we're not sure what's happening there.

MILTON MUELLER: So ODP is purely Board run and not community?

STEPHANIE PERRIN: Right.

TOMSLIN SAMME-NLAR: And it was delayed, I think. I believe there is a delay as well apparently due to uncontrollable circumstances. Yeah, that.

BRUNA SANTOS: Okay, I think we also can together try to see if we can find some more updates from the SSAD. There is a session today, as Adam is mentioning right now. But we can also try to get some more updates and share it on the list as well in the coming days if it helps everyone. Any other questions to Tomslin or about our policy discussions, anyone? Well, nice.

We have 12 more minutes to our meeting, and I wanted to kick start a discussion about hybrid meetings with you all. There has been a session this week. The session wasn't all too well attended. I wasn't able to be there because I'm a little sick and it was too late for me as well. But I wanted to maybe just get five minutes from you to listen if there is any input from our community about what we think about those hybrid meetings.

Do we think ICANN is able to do it? is there anything that NCSG should be doing in order to onboard our members into that phase of the moment we're all in? I wanted to hear from you if there are any thoughts or concerns about those hybrid meetings and whether or not we should gather a stakeholder position about them. Should we push or should we agree with the next meeting being a hybrid one whenever that's possible? Or should we continue to insist on remote meetings for the sake of participation? Because we also know that a lot of our community is also residing in areas of the world that did not quite have access to vaccines or might not be able to travel right now.

So I just wanted to hear from you guys if there are any thoughts or ideas or even criticism about this. So I'm opening the floor to whoever wants to take it. Milton, please go ahead.

MILTON MUELLER: So, Bruna, I have strong opinions about this but I'm wondering when you talk about hybrid are you just talking about the NCSG or about ICANN in general?

BRUNA SANTOS: ICANN in general. I know that community consultation is going to restart as it has in the previous meetings, and Org might want to know our position again. Like in the past opportunities we were a little messy in general terms of gathering our own NCSG position about hybrid meetings or going back to face-to-face ones. And we also know that there has been one broader community consultation in the past months that asked us things like, "Would you attend meetings unvaccinated people, or would you just attend meetings with only vaccinated people? Would you be okay with wearing masks?" I really wanted to get a sense of the room in terms of what would be our feelings with regards to a general ICANN hybrid meeting and so on.

MILTON MUELLER: Yes, so I do believe that we are in danger of unwinding and losing the ICANN community because of the absence of face-to-face meetings. I understand the concerns about safety, but I think we're just going to

have to bite the bullet and accept the fact that for the next couple of meetings not everybody will be able to attend.

But it's better to have hybrid in those cases than to continue to go along the way we are now where it's extremely difficult if I'm not in a location for me to focus on the ICANN meeting for more than an hour and a half. I'm in the middle of my office. I have other meetings, other people. I just can't really stay focused on ICANN. And I just get a feeling, particularly with respect to NCSG, that I'm completely losing touch with what you guys are doing and what I could be doing. And I would really strongly support having a hybrid meeting.

And just to let you know the context here at the university, we've pretty much gone back to normal. We wear masks in class and inside buildings. I realize in an international meeting it's more risky, but I think certain kinds of precautions related to distancing and masking is pretty good. And I think you might even see if ICANN could have vaccination capabilities at the meeting. That might raise some questions for them, but I think it might be something worth considering.

BRUNA SANTOS: Thank you so much, Milton. And I also see Adam and Caleb with their hands up. And I just wanted to point out that one of the conversations we were having these past days, especially with the council group, our councilors and group, was that we also needed to find an extra or a new strategy to reengage our members into the NCSG discussions. So if any of you, maybe Caleb or anyone else who wants to comment on that, would like also to bring some new ideas to that, that would be very

much welcome. But, yeah, I'm handing the floor to Adam and then Caleb.

ADAM PEAKE: Would you like to go the other way around? I'll follow up after Caleb, please. Wouldn't that be better? Thanks.

BRUNA SANTOS: Of course, yeah. Thanks, Adam. Caleb then.

CALEB OGUNDELE: Thank you, Adam, for the courtesy. I strongly [validate the opinion] that Milton already raised. This is about the time when we need to move on. [You agree with me] that I was one of the very strong voices that was against us going I think that was to the South American country which [again] this time around I do have some concerns for ICANN specifically.

That concern aside vaccinating at the site of the meeting, who pays for the testing? This is a question we need to—the PCR testing that is a travel requirement—we need to clarify this. Obviously, nobody wants to put additional costs on the travelers. On the other hand, I also do have this concern. But most people when they travel and get back to the country of origin might probably be asked to quarantine for a number of days. That is a concern.

The other concern I do have is the country where the meeting where the meeting we'll probably be holding, will ICANN be speaking to the country to give us some formal moratorium that says we don't need to

quarantine because of the meeting? Or will ICANN meeting be—I already know because it's a quarantine for 10 days and ICANN meeting is for another 5 days—so will ICANN meeting probably be 19 days? We need to get this clarification. We need to know where we are going. There is a lot of volunteer effort even in NPOC as well as NCSG. I'm pretty sure you can attest to that.

So these are just concerns that I do have. There are no solutions yet, but these are concerns that maybe we can debate on.

BRUNA SANTOS: Thank you so much, Caleb. And now Adam.

ADAM PEAKE: Thanks, Bruna. Hi, everybody. It's a little difficult to talk too specifically about this because on the staff side we feel that this is something that the SO and the SA leaders have been essentially leading on. We should be hearing from you. Of course, from Göran's point of view, and you'll hear him saying this, that he of course is concerned about asking staff to go in 150 or 200 people to meetings because he has to ask the staff to do something that not everybody is willing to do. I might be willing to travel, but some people reasonably because of conditions may not. They may have people at home that they have to consider.

So there are issues, but it has been discussed. And the plenary meeting a couple of days ago was quite good. So please take a listen because some of the questions that you're raising here were raised, of course, particularly around costs for support of travelers. If you've got to do a

couple of hundred dollars/Euros/pounds, whatever your currency may be, in COVID tests, then how is that compensated and so on?

And then there have been other meetings, and this is really what I want to come to. For example, last week the At-Large RALOs, the regional At-Large organizations, they held a call and invited Leon to come in and sort of lead a discussion about this. And some of the answers were quite interesting. People might not be willing to travel internationally, but they may be willing to travel nationally. Somebody crossing, you know, Milton, perhaps you'd be more willing. Not a good example to pick on a person, but perhaps somebody in the U.S. would be willing to go east to west coast rather than halfway around the world or something like that.

And that's really where it comes in with GSE. And, Bruna, happy to arrange a conversation with you later when it's easier for GSE to actually know where we're going with this to talk about what a regional meeting might look like from your perspective, what a national meeting might look like, what types of events we might do. Because, unfortunately, if you look at the COVID numbers growing in Europe—where you are now, sorry—they're going up. So we don't know what's going to happen this winter, do we?

But I think a lot of people are asking very similar questions and continue doing so. But we're very aware of how difficult it is to continue to keep people going when you're working like this. Somebody said that ICANN meetings are turning into a three-week meeting. It used to be you'd get on a plane and you'd do some intense work, you'd have conversations

that you couldn't otherwise have. But now it's spread over three weeks, and it is very hard. And of course, we know this because we're on the other side of it as well as staff. So perhaps early in the new year, later this year perhaps after the IGF experience which, of course, will be hybrid, we could have a discussion and take that forward. Be very happy to do that. Thanks.

BRUNA SANTOS: Thank you so much, Adam. And I was going to point out the IGF as well. I think it would be maybe one first experience for the broader Internet governance community and let us see what is going to come up from there. Let us see whether people will actually feel safe in attending. I also know that there are a lot of people like myself who are not too certain about going but might still be open to join being there and so on.

So let us see and let's just take a look at the IGF and see what will come out of that and then continue to facilitate these conversations among our community just so we're all on the same page and we all know and understand our concerns and what are the pain points for each part of our community and so on. So that's it. I see you have your hand up again, Adam, so I'm giving you back the floor.

ADAM PEAKE: Yeah, thank you. I should have mentioned the IGF. Which I'm a member of the MAG and I do so as a member of the technical…I'm technical community representative which I think means in many ways I'm also

a representative there for you. I'm not doing it as an ICANN staff member directly, and I've been co-chairing the working group for the MAG on designing the hybrid meeting for the IGF.

And I think the ideas that we hear for ICANN are quite similar. The idea that if you're participating online, you should be participating equally with somebody in the room. Which for the IGF means that we will all be using Zoom as our interface to a session. It doesn't matter where are. So you will use a raise hand function and whether you are online or onsite you will be in the same queue. These are the sorts of things that we will learn about.

The United Nations, of course, has the blue zone which is the zone where the IGF takes place. It essentially becomes a part of UN territory. So the requirements for COVID or COVID measures will be designated by the UN. And in the Palais des Nations, the Geneva UN building, for example at the moment that means masks will be worn at all times except when speaking. So at least you won't have to muffle through a mask when you're speaking.

But things like that. These are the things that we're going to be learning. And I'll put a link to the FAQ for the hybrid IGF. And if you have any comments or think there are questions that you might have there that aren't answered, then answer them and we will no doubt learn from it also in ICANN. So thanks very much.

BRUNA SANTOS: Thanks, Adam. And thanks everyone who joined this discussion as well. As we said, it's something we can definitely continue. And since we are two minutes past the top of the [inaudible]. And my idea for AOB was just to take the opportunity to thank Tatiana, Maryam, Raphael, and everyone who is actually leaving some of the leadership positions at our community.

And also Maryam for her outstanding work within NCSG, NPOC, and NCUC. I know, Maryam, you want to say some words. You want to maybe say your goodbyes or maybe what didn't work for you with us. And so I'm just going to hand you the floor and give you this opportunity to speak on that. But I guess that on behalf of the entire NCSG all I can say is a huge thank you, and thank you for all the support and help and for always being very patient to all of us in our requests. So, yeah, I'll hand you the floor right now.

MARYAM BAKOSHI: Thank you very much, Bruna. We're past the hour, so I just want to say thank you and I'll leave it at that. I'm sorry, but I'll follow up in an email. Thank you.

BRUNA SANTOS: Thanks, Maryam. Raphael, you have your hand up as well and so maybe….

RAPHAEL BEAUREGARD-LACROIX: Yes, it is very quick. Just to mention as well when I was talking about leadership transitions I forgot to mention that Ines Hfaiedh will be taking over Benjamin who was previously on the African EC seat. She will now be on the EC as well, and so that's a new addition to the NCUC team. So, yes, that's all for me. Thank you, everyone.

BRUNA SANTOS: Thanks, Raphael. Once again, it's really indeed sad that we are not able to say and give those goodbye hugs on a face-to-face meeting or even a hybrid one, but thank you all for being here. Thank you all for enduring for another NCSG meeting at an ICANN. This time ICANN72. And I will leave you all to get through the rest of your days or evenings. Thank you all for sticking around. That's it for me. I think we can [resume] this meeting. Thank you so much.

[END OF TRANSCRIPTION]