ICANN69 | Virtual Annual General – At-Large Policy Session: Beyond Budapest: The UN Cybercrime Treaty and DNS Abuse
Tuesday, October 20 2020 – 16:30 to 17:30 CEST

MICHELLE DESMYTER: Thank you. Hello, and welcome to the At-Large Policy Session: Beyond Budapest: The UN Cybercrime Treaty and DNS Abuse. My name is Michelle Desmyter 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 I've noted in the chat. I will read questions and comments aloud during the time set by the Chair or moderator of this session.

Interpretation for this session will include Spanish and French, and will be conducted using both Zoom and the Remote Simultaneous Interpretation platform operated by it by Congress Rental Network. Attendees are encouraged to download the Congress Rental Network app, following instructions in the Zoom chat or from the Meeting Details document available on the Meeting website page.

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 the language that you will speak if speaking a language other than

English. Please also speak clearly and at a reasonable pace to allow for accurate interpretation. Please mute your microphone when you are done speaking. When speaking, please be sure to mute all other devices, including the Congress Rental Network application.

With this, I will hand the floor over to Joanna Kulesza. Please begin.

JOANNA KULESZA: Thank you very much, Michelle. Thank you for joining us during this session. We do have a few slides. I have a few slides. If we could get them on the screen, that would allow me to give our guests, our speakers today a just introduction.

The title of the session, as highlighted in our agenda—and I agree, I admit it—it was deemed to be controversial. We're looking beyond Budapest and having the head of the Budapest Convention join us here today. It makes it even more controversial. We're trying to look beyond Budapest to see what are the current, ongoing, and future legislative international processes that are targeting malicious activity online.

We here within At-Large have held a number of sessions and have tried to be active participants of the discussions going on within ICANN on DNS abuse. As ambiguous as the notion would be to non-ICANNers, it is quite clear to us what we mean when we discuss DNS abuse and the At-Large has put in a lot of effort building capacity on DNS abuse.

This session is yet another attempt of us trying to better understand what DNS abuse means and how to effectively protect end-users. Were trying to look into existing instruments that are trying to achieve the same goal, and we will also explore future possibilities to make DNS abuse a topic for the entire community, finding a way that we can effectively combat it. If we could move to the next slide, those are very basic slides. I just have the agenda and a very brief introduction into our discussion here today.

I will start us off with a recap of the discussions we've had. Here within At-Large, we have looked at various geopolitical trends that focus on international policies that might impact the ICANN community. We've looked at the work around UN, and I will provide us with a very brief introduction and a freeze-frame on where we stand within those geopolitical discussions.

Then my ALAC EURALO colleague will give us an end-user perspective. Matthias has kindly agreed to be the case example of an end-user facing the challenges that DNS abuse policies might bring to individual end-users as applied.

And then finally, as already said, I'm really glad that Alexander Seger agreed to accept our invitation here today. We just have 60 minutes and we've reserved quite a large portion of that time for discussions. So I'm very much looking forward to Alexander giving us an insight of similarities between DNS policies and existing, precise, specific, and fully functioning international processes that are targeting the very same aim: keeping Internet end-users safe. I will proceed to the next

slide just to give you a glimpse of the background where we're come from, what this discussion is all about.

The next slide, if we could proceed is obvious to everyone who's participated at recent ICANN meetings. We keep discussing the DNS Abuse Framework, a non-binding document of policy that's being developed by those on the frontline of fighting online abuse. If we could move to the next slide, please. I just have the definition here of DNS abuse, something you will find in the framework and something that I know my colleagues, our distinguished guests, will also look into.

We have certain activities defined as harmful to the network DNS abuse and therefore covers notions such malware, botnets, phishing, pharming, and as we've explored here within At-Large most controversially, spam. If we could move on, you would see a more specified definition. Yes, to the next slide. Thank you very much, Michelle.

You will see more specific definition of DNS abuse and the actions that are expected of registrars and registries when attempting to keep the network safe. As you can see here, there is a clear leap into content and an encouragement for registries and registrars to act even when there is no judicial decision. Just a specific incredible notice should be enough for registries and registrars to act to keep us safe.

Now, all of these, I would like to put in the context of the following slide that introduces Alexander and that links this introduction to his

presentation. If we could have the following slide, I'm just going to give the headline of the Budapest Convention. I know that everyone in Europe is well aware of what the Council of Europe does. I'm certain Alexander will give us a very brief intro. I'm not so sure that this is everyday knowledge to our colleagues and partners from outside Europe, so I welcome this opportunity to spread the word around the ICANN community why the Budapest Convention is the greatest achievement we do have in fighting international cybercrime. I do want to link this discussion to discussions we've had on geopolitics within ICANN.

If we could move to the following slide, you will see something we've discussed here before we've had the ICANN Org reps give us various updates on what's going on in the United Nations. Now, it seems as if currently the United Nations is so fascinated and excited with the success that the Budapest Convention has enjoyed, they went to have one of their own.

Now, this is not something that's happening right now and it's not something that's going to happen tomorrow. But when we did have our geopolitical discussions, we talked about how the community might want to get involved into those processes to better represent and to better protect end-user interests. So again, this is a policy discussion around those outside trends, if you will, that we might want to get involved. And the whole point is for us to try to figure out whether it makes sense, and if so, how we might want to do it.

Now, on that last slide that I have is the direct link between this discussion and geopolitical discussions we've had before. If we could move to the next slide, Michelle, that would be wonderful. Oh, right. That is the paper that you will find here on the ICANN Org website produced by ICANN's Government and Intergovernmental Organizations Engagement team that discusses currently UN developments, how they might impact the work that we do here within ICANN. I welcome Veni who took the time to participate. I know, Veni, you will be presenting this paper tomorrow during a much rather longer session on platforms. So I encourage everyone who's joining us here today to listen in also tomorrow on the discussion of platforms and regulation. But we did use Veni's wonderful, very informative paper as a link between current, ongoing international processes and DNS protecting it and the notion of DNS abuse.

I think I have one more slide that just basically introduces Matthias. These are the scoping questions we will try to answer during the session, and I will ask Matthias to give us an example of how an end-user might approach these. So we will try to figure out if there is a link between DNS abuse and the cybercrime laws as we have them right now on the international arena. Is there a role that ICANN community might play in those international discussions? And finally, has law failed? Are we down to policies and the standards that we develop as ICANN because International law has little or nothing to offer? Yes, I'm trying to be controversial, and you know that's something I tend to do quite often.

With that, I'm going to stop. I'm going to hand the floor to Matthias. I know, Matthias, you will follow suit and you will also try to be controversial, which I embrace and welcome. With that, I give you the floor. I am being told we need to stick to time. I've been talking a little over my 10 minutes so I'm just stopping right now. The floor goes directly to Matthias, and then I'm going to ask Alexander to respond or to give us more details on what are the tools we could actually be trying to explore. I'm going to stop. Matthias, The floor is yours. Thank you.

MATTHIAS HUDOBNIK: Hello, everybody. My name is Matthias Hudobnik. For the folks who do not know me, I'm a legal engineer and one of the members of the At-Large Advisory Committee. As Joanna already nicely pointed out, I will try to emphasize on the current legislative processes and their impact on to ICANN's DNS abuse policies and what to expect. The implications are embedded in a practical example from an end-user's perspective, of course, and my talk will be as brief and practical as possible so that we have enough time for a fruitful discussion afterwards, which I'm sure we will have. Next slide, please.

This is Matt. Matt is an Internet end-user. And as you can see in the picture, he has his own domain, www.Matt.info. He lost his domain, obviously. But one day, his domain got abused. Matt is very concerned about this criminal act. Please go to the next slide.

What do you think will Matt perhaps do as unusual Internet end-user? In general, I assume he might report it to the local police and they will usually act under the domestic criminal and/or other specific telecommunication laws, which are more or less the same in the respective legal systems, taking into account if it's a common law, civil law, or mixed law system. If the criminal act might have a cross-border relation, which is quite often very likely in cybercrime cases, this case might be coordinated by a cooperative police or a law enforcement effort like in Europe, the European Union Agency for Law Enforcement Cooperation and under their mandate and the legal regime of the Europol regulation. But as I said before, the origin legal basis of the investigation is usually grounded under domestic criminal law. When the suspect resides in a foreign country a mutual legal assistance, so-called MLAT request, is commonly used to formally interrogate a suspect in a criminal case. Next slide, please.

So let's go a step further. As you can see here on the very controversial picture, the picture is censored. Let's assume the Internet end-user Matt has this picture on his website because he's a journalist and the ones who draw their attention to an event, which is, by the way, a real-time example, so the censored picture is called Napalm Girl. This picture was made on June 8, 1972 and it's a photo of South Vietnamese forces following after terrified children. In the middle there is a nine-year-old Kim Phúc (the name of her) and this picture also was winning the Pulitzer Prize. There was a heated debate about freedom of speech in Norway after and Facebook deleted it from a Norwegian author's page. So Facebook said it is child porn and took it

down because it violated the site standards on nudity. A little known team of humans, not algorithms, Facebook decided to remove this iconic photo from the site. The shown sense of picture would violate ICANN's Expect Standards of Behavior and this brings me back to Joanna's introduction. Please, the next slide.

As Joanna already pointed out, we are discussing various legal frameworks of different levels and, in particular, I want to point out to the DNS framework, which is signed by 48 signatory registries and registrars that are bound by these principles. And the particular point in this paper, which I want to point out is, when should a registrar or registry act on website content of news? And in particular, what I want to highlight is the fact that in this paper, it says that the registry or registrar should do this without a court order. I will not repeat here the things which are written on it but what strikes me in particular is exactly this wording, but I will come to it a bit later.

Down after the picture, you can see a scale also from the paper which shows the policy that can remove content before it escalates to the reseller, if there is one reseller involved, the registrar and the registry. So the paper also points out that a registry or registrar can only disable an entire domain name and complainant should work first with the site operator, the registrant or the host provider to remove the content rather than causing potential collateral damage by acting wild the DNS.

So these are very interesting points to me and I do not want to dive into a content discussion or a discussion about the [NGO] service Act

because there will be an extra session coping with these issues and this is out of the scope of this session. Rather, I want to talk about the definition I wrote on this slide.

So what does this might mean for Internet end-user? And how does this affect the end-user? I just tried to draw a picture again in a very practical way, I would say, from an end-user perspective. So one can say, "Oh, that's fine. I can just contact my registry or registrar who might act for me without a court order to disrupt the form of my website content abuse as stated in this paper."

On the other hand, you could also argue why do we have all these legal frameworks and regulations embedded in our legal systems, including independent churches who decide and are educated for their capacity? In doing so in an independent manner and in one or, I would say, in more or less effective way. Of course, you can argue this. The next slide, please.

So what I wanted to say—and I comment again—don't get me wrong, I'm not here to solve this problem. Either I'm here to say that we should not think about additional remedies to tackle these abuses, but I think it's crucial to talk about it. And I want to point to potential advantages and disadvantages, depending of course for where are you coming from.

So as you can see here on the slide, the question which really interested me were, how can we still guarantee fundamental rights, like freedom of speech, if we agree on such DNS remedies? Or how can

we tackle the problem of end-user DNS abuse, realistically, but still having safeguards implemented that prevent misuse or censorship by these decision-makers? Should there be a supervisory body or a body? When yes, who will review it and how will we make the initial decision review? And also who will concretely decide at the registry or registrar level, and to what capacities? And the last one, how will the decision-makers gain the respective skillset if we agree on such remedies?

So with this, I want to stop. I thank you and I'm very much looking forward to your input and a fruitful discussion. Thank you. I'm handing over to Alexander.

JOANNA KULESZA: Go right ahead, Alexander. Thank you, Matthias. The floor is yours.

ALEXANDER SEGER: Thank you. A very, very interesting discussion that was far beyond the 60 minutes allocated this afternoon, but I hope I can stay further involved in the dialogue with you. Indeed, the title of the session was a bit provocative, but it's fine. I would say it's not a question of beyond Budapest, it's a question with Budapest we can come to global cooperation on cybercrime, including DNS abuse. For those who wonder what Budapest means, it's a Budapest Convention on cybercrime opened for signature in Budapest in 2001. Next slide, please.

If you look at cybercrime and the Budapest Convention, if we look at the global framework for cooperation and cybercrime—and here we look at DNS abuse as a matter of criminal justice—the starting point is that governments do have a positive obligation to protect. It means government should not only refrain from not violating rights, but governments have the obligation to protect individuals against crime, including through criminal law. And you can find a very important decision in this respect that also refers to the Budapest Convention by the European Court of Human Rights of 2008 in a decision K.U. versus Finland. A very important decision.

Cybercrime and matters of electronic evidence. Any crime, by the way, may involve electronic evidence that require an effective criminal justice response. And this is what the Budapest Convention provides.

It is not a national security instrument. It is not an intelligence gathering instrument. It's about specified data needed in specific criminal investigations. And since Matthias referred to the rights of individuals and how to protect them and safeguard such rights, we have to keep in mind that a criminal justice response is protected. Yes, there are powers to investigate and prosecute to protect individuals against crime, but these powers are limited by rule of law, conditions, and safeguards to protect the rights of individuals, including suspects, and to prevent abuse. Very important.

We should also keep in mind that, of course, the criminal justice response cannot solve all problems, cannot prevent and do something about all forms of DNS abuse, but it's part of the measures to prevent

and respond to security threats. Criminal justice response is one important part of a much broader response. Next slide, please.

Now, as much as also underlined, we have to be very careful that with whatever we do, we do not unnecessarily entrench freedoms on the Internet. If you look at the Budapest Convention, the starting assumption is the free Internet, which means the Internet information flows freely and individuals can access data and share information. But there is also the obligation to protect by governments and restrictions to the free flow of information on the Internet have to be narrowly defined in criminal law in line with rule of law requirements. It's very important. This is the rationale of the Budapest Convention. The idea is if we expand the scope and the geographical reach of the Budapest Convention worldwide, we are quite far with that already. So that's, on the one hand, what we have in the Budapest Convention.

Then there are some counter-proposals floating around. I'm not saying that this is specifically what the UN Treaty on crimes committed via information communication technologies will be about. But there was proposing such a treaty come up with such ideas. Their focus on information crimes, not cybercrime but information crime, based on the doctrine of information security, underlying idea is that governments have sovereign control of their information space. In that sense, governments also control what information individuals should be exposed to. Concepts of crime rather vaguely defined safeguards are limited, and because such an approach is probably not consensual globally, the outcome or the risk may very well be that the

outcome may be further fragmentation and spheres of influence, rather than a global response to a common threat. That's the risk that we see, that we hear from parties to the Budapest Convention and we discuss with them. Next slide, please.

What is the Budapest Convention about? It's about governments. Basically, the parties have to do three things. They have to provide in the criminal law for specific offenses against and by means of computer systems with any offense is a limited list. They have to provide their criminal justice authorities with procedural powers to investigate cybercrime and collect electronic evidence in relation to any crime. And they have to engage in effective international cooperation on cybercrime and any crime involving electronic evidence. This treaty is almost 20 years old but supplemented by guidance notes. I will explain that in a second. It's notes that are adopted by the parties to the convention to say, "Okay, this is how we apply the provisions of the convention to more recent phenomenon." And currently, a protocol is under negotiation on enhanced cooperation on cybercrime and electronic evidence. I'll be mentioning that in a minute.

The Budapest Convention is a framework. You can think about it like a triangle where you have the Budapest Convention and related standards, a number of other standards that we make use of, the data protection standards convention, [inaudible] convention, the Protection of Children against Sexual Exploitation and Abuse and others. Then we have the Cybercrime Prevention Committee, which is

the parties to this treaty that I represent there. I'm the executive secretary of the committee. And then we do capacity building through Cybercrime Programme Office that supports countries worldwide to beef up the criminal justice capacities to build the cybercrime electronic evidence. The Budapest Convention is all of this. It's a mechanism, not just the treaty, and the concept of "I'm in charge of this." We now have 65 parties and another 12 states that have signed. They've been invited to accede to the Budapest Convention. Next slide.

If we look at it in connection with COVID-related cybercrime—phishing, malware, ransomware, DDoS attack, spam, fraud, and so on—you find all of these phenomena covered in the substantive criminal law articles, meaning a conduct that is criminalized often in combination of several of these provisions. But there are guidance now that shows how you can use different provisions to address DDoS attacks, malware, spam, and so forth. So in a way, all of these is covered in one way or the other, which means parties that have implemented to put up this convention, the parties have criminalized, have proven law means to go against this type of COVID-related cybercrime and DNS abuse. In addition to that, the procedural powers of the Budapest Convention to investigate, secure evidence, and then prosecute, and convict offenders with safeguards, Article 15 rule of law safeguards, and then there are guidance notes also that explain further how you can use procedural powers. Plus there is a framework for international cooperation or you can also cooperate internationally against this type of offense. So the framework is there,

you cannot say there is not enough criminalization. At least in the parties to the Budapest Convention, this type of abuse is criminalized. The means are there to investigate and cooperate. Next slide.

As I said, we have currently 65 parties. The most recent ones we are Peru and Colombia. A number of other countries have been invited to accede. Just a few weeks ago New Zealand was invited to accede. Now you see that it's completing its domestic process to become a party. Not just European countries, but also in Asia. We have Philippines, Japan, Sri Lanka. In Africa, we have Ghana, Senegal, Mauritius, Cape Verde, and other set of parties. The United States, Canada parties, Costa Rica, Argentina, and many other countries are parties. It's not a European instrument. It's very much a global instrument. But in addition to those 77 states that are about to become parties, at least double that amount, double that number, have used the Budapest Convention to put the domestic law in line with this treaty. We now have 107 or 108 states worldwide that have criminalized conduct in the domestic law proceed in the Budapest Convention. That's very important to understand. Next slide, please.

Now, as I said, there's a new protocol underway. We started three years ago in September 2017. We hope that very soon we will finalize the negotiations and there are a number of other things to be done, and then we can have hopefully open this protocol for signature in 2021 next year. So a year from now, that's it.

Why is this protocol needed? Because the scale, the quantity of crime, users, victims, devices involved, they're very important also because

of this problem of territoriality and jurisdiction. As Matthias said, the powers of law enforcement are limited to the territory of the law enforcement. If you want to get evidence from somewhere else, from abroad, you have to do it normally via mutual assistance, which takes time. And if you don't know where the attack comes from or where the data is, you don't know where to go to. So, because of this rather complex problem of territorial jurisdiction, there was a decision that ended up sometimes not sufficient effectiveness of mutual assistance when it comes to volatile data. The need for a new protocol, it came up and it started three years ago. Next slide. Next slide, please. Thank you.

Now, very briefly about the elements of the protocol. I'm afraid I cannot go too far with this. It would take too long, and because some of the issues are still under negotiations. But there will be in this protocol normally provisions for more efficient mutual legal assistance. How can you make this whole process of obtaining data in government to government relations in a more effective way, more efficient way, more timely way so that you can then also obtain evidence and continue with your judicial process? It's very important.

There are likely to be two provisions on expedited cooperation and emergency. One is through emergency mutual assistance so that also on a weekend when normally Ministers of Justice and prosecutor general's office are closed, you can still get mutual assistance between parties to this protocol. But there's also another provision where countries can use their domestic procedures to obtain content, not

just subscribe information, but also traffic and content in an emergency and disclose it to the authorities of another party if it's a matter of life and death. But this may be very important provisions on emergency cooperation.

Then very interesting one is the idea that authorities of one state of one country can directly cooperate with a service provider in another jurisdiction, in another party. Today I'm in Bucharest in Romania, so Romania needs data from Mauritius that they can cooperate directly with the service provider in Mauritius or United States or wherever the other party is. And for that, we have already published some time ago a draft provision to this where you can go directly to a service provider in another party to obtain subscriber information. With a range of safeguards—it's not a free-for-all—there are safeguards, there are clear rules to obtain subscriber information foreseen in this provision. Then there is one—and this is very interesting probably for the ICANN community—we are considering whether we can create a legal basis for request to the disclosure of WHOIS information by registrars and registries. This is currently under negotiation. We hope that soon we will have a draft. And then we will make it available and seek also the views of other stakeholders in this. This is not to replace what currently is being discussed in the ICANN context. It is to complement, to provide a legal basis for whatever mechanisms, procedures, rules come out of the ICANN process.

And all of these, of course, if you go into expedited cooperation emergencies, the data is quickly disclosed, if you go to direct

cooperation with service provider, if you go to direct cooperation for disclosure WHOIS information, then we need to have strong data protection safeguards also in this protocol. It is compatible of course from a European Union perspective with the GDPR, but it is also compatible with the legal systems of any other country that will become a party to this protocol. These are very complex discussions, sometimes frustrating, but I do believe that within the next few months we will be there and it will have a draft protocol, and hopefully this will be available next year open for signature. And the last slide please. One more. The conclusions.

Whatever happens in other forums, UN context or elsewhere, we believe that the Budapest Convention, particularly with its future protocol, it's likely to remain the most relevant international agreement on cybercrime as a matter of criminal justice. The offenses involving DNS abuse are covered by the convention parties to have that in their criminal law. The procedural international cooperation provisions of the convention are available to investigate and prosecute DNS abuse. As I said, discussions are underway, including a legal basis for requests for and disclosure of domain name registration information across parties to this protocol. So I cannot provide more to it on what is going to be in this WHOIS provisions. It's not yet finalized, but hopefully soon we will have a draft available for public discussion and feedback from stakeholders. Thank you.

JOANNA KULESZA: Thank you very much, Alex. That was very informative and inspiring as I can see by the questions popping up in large numbers in the chat. I've taken down the questions. Some of them regard your capacity building activities. We would love to hear more about GLACY+. Some of them deal with specific aspects of implementing the convention. I know you have comprehensive answers. So what I would like to do is I would like to give the floor to the first hand up we have in the room that comes from Hadia. If Hadia is able to speak, I would be willing to give her the floor just to hear feedback from our participants. Then I would love to go through the questions, I'm taking them down. I'm going to ask Alex, whether he wishes to address them one by one or in bulk. And then I encourage you to raise your hand, as Hadia did, and take the floor interacting with other speakers. Hadia, the floor is yours.

HADIA ELMINIAWI: Thank you so much, Joanna. My question is in relation, actually, to what has been just presented. The convention is actually the only international abiding treaty when it comes to cybercrime. And it definitely aims to protect the society against cybercrime by adopting appropriate legislation but also by fostering international cooperation. My question is in relation to the international cooperation part. When it comes to DNS abuse-related matters or DNS-related cybercrime, and as we can definitely see that are criminalized by the convention, can ICANN act as a regime for this international cooperation? That's just a thought. Because again, it's obvious that what they're talking about in relation to DNS abuse is

criminalized. But then the problem is actually the actions that need to be taken. So again the question is in relation to ICANN and if actually it can be a regime through which such cooperation can happen. And especially, for example, if we look at matters like WHOIS or registration data, and already the community is working together on such matters. Thank you.

JOANNA KULESZA: Thank you very much, Hadia. Alex might find it useful for me to refer to your experience with the EPDP (the Expedited Policy Development Process) that was focused on, well, let's call it WHOIS but it's not as much WHOIS as it is the GDPR implementation. So Hadia has been very active in trying to maintain ICANN on point when it comes to those international consensus building processes. If possible, Alex, I would appreciate you addressing the specific question, and then we can move to the long list of questions that I have here that refer to the various aspects of the work that the Council of Europe is doing. I need to be mindful of the time, so I apologize in advance if there are any questions that are missing. Alex has kindly indicated he would be willing to support us further. So I'm certain there's a channel of communication we can open up for this collaboration to persist. Alex, if you would like to take on Hadia's question first, and then we can move to the others, that would be wonderful. Thank you.

ALEXANDER SEGER: Thank you. Organizations like ICANN include the justice authorities or registrars, registries, service providers in the broader sense of the private sector. Of course, they should cooperate and there's a lot of merit in cooperation with criminal justice authorities. But when it comes to criminal justice action, making decisions, it should be left with criminal justice authorities.

And I think what we have here in this EPDP process, WHOIS, and so on, I think that's a good example where hopefully there will be an effective mechanism, procedures coming out from that process for access to a disclosure of WHOIS information. But still authorities need a clear legal basis in their domestic law to act. And that's what we are trying to attempt through the Budapest Convention. Again, it's very much a cooperative effort, but I strongly believe that criminal justice action should be left to criminal justice authorities.

JOANNA KULESZA: Thank you for making that very clear, Alex. Thank you. Matthias, I am going to give you the floor for feedback, but as I already said, I'd like us go through the questions that appeared. Looking at them in chronological order, the first comment or question came from Judith Hellerstein. Thank you for raising this, Judith, and I know Alex will appreciate this as well. Could you give us a very brief recap on the work that's being done around GLACY+. Within At-Large, we have a very strong, a Fellow community. They are very active when it comes to capacity building. If we have any members of a Fellow here in this meeting, I'm certain they would appreciate a succinct yet informative

feedback on the work that you guys have done in terms of capacity building cybercrime, the Budapest Convention, and I would argue a spillover effect that you guys have been enjoying even in countries who have not officially ratified that convention. Would that be possible, Alex?

ALEXANDER SEGER: Sure. Okay. In 2013, they decided to establish a specific cybercrime program office that is doing only one thing, supporting countries anywhere in the world in the strengthening of the criminal justice capacities, from strengthening domestic legislation to training, to many other things. And that office is based in Bucharest in Romania. So that was created in 2013, beginning operation in 2014. And we have a number of programs running but for countries in Africa, Asia, Latin America, Caribbean, Pacific, and so on, the GLACY project, Global Action on Cybercrime Extended. Because it's now in second phase, GLACY+ project. It's a joint project of European Union and the Council of Europe. There's quite a large budget, 19 million Euros. They're discussing further increases there. And through that we can support any country.

Now, there's so much demand that we focus on countries that politically have committed to join the Budapest Convention. That's why we provide the full menu of activities, training, and everything else that goes with it now in Nigeria, in Ghana, in Senegal, in Mauritius, and so on. However, they can also support other countries strengthening the domestic legislation and associate them with some

other activities like Namibia, like many others, Congo and so on—we're also working with them—Fiji, Samoa, and many others. But for the full menu, we require a political commitment to join the Budapest Convention. So that's the rationale of that. We are working with about 140 countries, I believe, right now under GLACY and other projects.

JOANNA KULESZA: Thank you very much. That is very informative. Again, I know that the Council of Europe has a very efficient office and staff that will be looking forward to providing you with more information.

We have two questions that have taken down. I have noted from Stephanie Perrin again, a very active ICANN community member, a very distinguished ICANN community member focused on prioritizing both privacy and security. So those questions do refer to privacy standards. Stephanie asks, "With respect to safeguards, why not insist that those who wish to sign the Budapest must also sign on to Convention 108?" And if I may, I think it makes sense to link it with Stephanie's second question, "In terms of jurisdiction, will there be a data protection oversight office such as exists in Europe in Eurojust? Similar problems, with respect to needs of data protection oversight solution should be addressed."

I'm curious if you might have any wise words for the privacy advocates within the ICANN community who are always concerned about the need to prioritize both security and privacy. I understand this is where the questions from Stephanie are coming from and it would be

wonderful if we would get your feedback to cybersecurity, the cybercrime guy, on those privacy concerns. Thank you.

ALEXANDER SEGER: Okay. I'm happy to respond to the question, but let me also make another remark in this context. I made—I think it was like the second or third slide—this point that criminal law is protective. The reason why you have criminal procedural law is to regulate how governments, how public authorities can interfere with the rights of individuals. So criminal law is protective. We have to be very clear on that. There are lots of safeguards in place apart from the data protection requirements for criminal justice authorities. Let's be very clear on this.

This is less the case, in my opinion, when it comes to national security bodies. A big problem that we have after some scandals, some revelations about what national security institutions are doing, the result is more restrictions for criminal [inaudible] and not necessarily for national security. It's a very weird and dynamic that we see. To come to Convention 108, [inaudible] or 108+ as it's now in the modernized form. It's no coincidence that many of the non-European parties to the Budapest Convention—Mauritius Senegal, Argentina, and others—are also parties to Convention 108. It's very important. I mentioned that currently we are supporting through GLACY+, we're supporting Namibia in the reform of the cybercrime legislation. But along with that, we're also supporting them in the reform of the data protection legislation. Similarly we've been working with Sri Lanka,

we've been working with Dominican Republic, and many other countries along those lines. So we're very much in favor of it.

In the protocol to the Budapest Convention, it's very difficult to negotiate. We're now trying to take the standards and proceeded in the protocol itself. So not just cross-reference to other standards, but have these standards in the protocol to the Budapest Convention itself. And of course one of the essential such sub-provisions of the data protection article will be on supervisory authority. So it would be required that parties to the protocol will also have data protection supervisory authorities in place to make sure that the rules are respected in that given party. So if now one party transfers data to another party, that party can be sure that the data is protected at a similar standard in the receiving party.

JOANNA KULESZA: Thank you, Alex. Moving on swiftly, we have 12 more minutes. Again, we're doing the housekeeping. We have more general questions, I would say, from Olevie Kouami who asks, "What is the state of relationship between the Budapest Convention and the Malabo Convention?" I'm curious if you might be willing to share your thoughts on that. I'm assuming the question is targeting Alex as well.

ALEXANDER SEGER: The Malabo Convention of the African Union, in some ways was much further than the Budapest Convention. The Budapest Convention, criminal justice. The Malabo Convention has data protection and it has

ecommerce in it. It is also cybersecurity aspects in it, and so forth. So we only have to look in this regard to this question it's, what is the relationship between the cybercrime part of the Malabo convention and the Budapest Convention? Because the other part is outside the scope of the Budapest Convention. And here we have discussed this and analyzed this in great detail. We have had many discussions. We have good cooperation with African Union in this respect. We see this as perfect complementarity because the Malabo Convention is limited to Africa, cannot cooperate with United States or with European countries under the Malabo Convention. It's only within Africa. It does not have specific provisions and international cooperation in it. It has a limited number of procedural powers to secure electronic evidence, but there is a strong commitment because it was adopted by the Heads of State in the government of African Union Member States. So we have an agreement with the African Union Commission that we, together, promote implementation of the Malabo Convention and the Budapest Convention on the African continent.

JOANNA KULESZA: Thank you, Alex. I have a more general question again coming from Siva. "Could there be a cross-jurisdictional judicial, responsive, swift process?" I think you might have an answer for that one. A swift process. Sorry, Alex, can you hear us all right?

ALEXANDER SEGER: Yeah, but I don't know what it means.

JOANNA KULESZA: Can we enforce laws quickly? I'm reading into Siva's question. Can we do this quickly and efficiently?

ALEXANDER SEGER: Okay. There are in the Budapest Convention currently a number of measures in it that permit immediate action, like you need the other preserved in another party a phone call, an e-mail, and they can be preserved within hours. And several provisions of the current Budapest Convention Article 29 and 30 in particular, and the system of 24/7 contact points. In this future protocol, there will be some provisions that will probably go further than that, namely, that you can go directly to a service provider in another party and to obtain at least subscriber information, again, with a number of safeguards that they have been building.

Last, there are a number of provisions that will be in the future protocol that will provide for a more effective execution of production or this in the other party to cut an MLA process that would take 10 months, I think, as Matthias mentioned in one of the slides that will cut it down to maybe a few weeks. Still too long. If there is an emergency happening, whether it's a terrorist attack underway, the very negligent access to data in the other party to figure out who are the others involved with this, the more attacks coming, like what happened in New Zealand, what's happened in Paris, Charlie Hebdo, and so on. For that, we also put the two provisions in place that allow

you to very quickly get access to such data in emergency situations. So yes, there will be means to have more effective action, criminal justice action. These safeguards are very important foreseen in the protocol as it is, in the Convention as it is, but also the future protocol.

JOANNA KULESZA: Thank you, Alex. Another question, an open-ended one, I believe, not too challenging, comes from Judith. Thank you for posting that question, Judith, to clarify things. "Do countries need to sign to all additional protocols when they accede to the Convention, and how does that work?"

ALEXANDER SEGER: No. You cannot join a protocol if you're not joined the convention first. But you can join the convention without joining the protocols.

Let me give you an example. There is a first protocol, actually, only so far but we're now working with the second protocol. The first protocol from 2003 was from xenophobia and racism permitted by a computer system. Very important for African countries, very important for European countries. It's also by South African at the time participated in the negotiations. But in some countries, United States is one of them, freedom of speech is so highly protected that they said, "We cannot join this protocol." So United States and many parties—I think the protocol is now about 35-36 parties. The convention has 65 parties. So you see 30 parties separated by the Budapest Convention are not parties to the first protocol. I believe that for the second, for

this future protocol, because it has very attractive features in it that all of us need to have a legal basis to access WHOIS data, to have the possibility to direct incorporate the service for the [missed] safeguards—very important—I believe that this second protocol will make it more attractive format, many other countries will join the convention. But they have to join the convention first, and immediately after that they can also join the second protocol. But they don't need necessarily to implement the first protocol.

JOANNA KULESZA: Thank you, Alex. That was very clear. I think this is something that also we had in the comments coming from Michael Graham, who emphasize to the list we have here for DNS abuse should include other illegal acts. And he mentions here clearly privacy rights or freedom of speech violations. We talk about hate speech, which is always challenging. But not to get into the discussion on the merits, again, I'm looking at the clock. We have five minutes. What I would like us to do. I have four more questions. With the permission of our panelists, I would go through these then I will let you guys respond making your concluding remarks. I have been warned that if we go over time, there's going to be a death penalty on all participants, so I'm not taking that risk.

ALEXANDER SEGER: Human rights.

JOANNA KULESZA: Yeah, right. We shouldn't have that, should we? But that's ICANN. You're welcome, Alex. So I will just go through the questions and then I will refer to our panelists for a brief summary, hopefully some feedback. I welcome your willingness to engage with us, Alex. We're really glad to have you. Let me just go through the questions and then I'm hoping to be able to reserve a few minutes for your feedback.

Question coming from Elizabeth, "RE: legal basis for requests for the disclosure of domain name registration information across parties to this protocol. By parties, we mean governments, not individuals or non-governmental entities?" There's a question mark at the end there.

Another question coming from Siva, "Creative great minds from judiciary and law order should be able to come up with interesting proposals, why talk about cynicism at inception before even the thoughts are generated by think tanks, for instance?" So an invitation to more creativity, I understand.

Question coming from Rick, "The U.S. Federal Trade Commission has seen an increase in online consumer fraud around the COVID-19 pandemic. Has the lack of access to WHOIS data due to GDPR hindered law enforcement investigations and enforcement?" That's the end of the question.

A question coming from Zakir, "Thanks for the useful discussion. My question is for Alex. Since there is a heated debate going on about the UN Treaty on Cybercrime proposed by Russia"—I think Alex will be able to refer to the content of that proposed treaty by Russia—"which

has already got considerable support. Do you think that both, the UN Cybercrime Treaty and Budapest Convention with its new protocol will co-exist or go side by side?" I take the blame for the confusion behind the two instruments and I'm happy to provide details why we put a UN Cybercrime Treaty in the headline. There's a cybersecurity discussion we've discussed here within ICANN, and there's a cybercrime discussion that is just being initiated.

And one last question, "On the last bullet point on your last slide discussions on legal basis of the protocol for request with regard to the WHOIS data, Alex, did you mention consultation of various stakeholders within ICANN to collect/confront/consolidate views on this? If so, in what form and what timeframe?"

These are our questions. We have two more minutes. I'm going to give Alex one more minute to try and give us just an emotional feedback. We hope we made you feel welcome. The questions show great interest, but I'd like you to give us a very brief feedback. And then I would like to go to Matthias for a concluding remark. Thank you.

ALEXANDER SEGER: Okay. So the first question was about the future protocol legal basis access to WHOIS and who can access them. The Budapest Convention is a criminal justice treaty. We have to remain without our competencies, we cannot regulate for others. And indeed it's the legal basis for criminal justice authorities to request data. That was the first one.

Creativity, yes. We need creativity. I believe criminal justice terminology is extremely conservative. It's very difficult to remove anything. You're still working on the lotus decision when it comes to jurisdiction from almost 100 years ago that defines jurisdiction concepts internationally. So we are very creative now I think in creating international law through the protocol to take this further.

From what I understand from law enforcement practitioners, yes, there is a huge amount of COVID- related cybercrime. It's a massive spike that we see. There are all forms of it. Part of the problem in investigating it may indeed be the lack of access or limited access to WHOIS data.

The UN Cybercrime Treaty, we're not sure but it can be called a Cybercrime Treaty. Maybe it will be called an Information Crime Treaty. We don't know yet what is going to happen there. There are other treaties where the UN has treaties but the Council of Europe has other fields of work—corruption and many other areas, money laundering to some extent. Of course, they can co-exist but we don't know yet what will be the content of the UN treaty countering crimes committed by information communication technologies. I think that's the term that is used there right now.

And regarding consultations on the protocol we had last year about a year ago last year in end of November, we had a first round of consultations. At that time, it's not yet about the WHOIS proposal in the protocol. It's about other elements. ICANN represent this where there are many, many people were there, about 450-460 people. We

have to discuss now within the negotiating parties, between the parties, it is likely that once the WHOIS proposal is out in public that we will invite comments, but we have definitely foreseen that in the beginning of next year, when a draft of the whole protocol is available that we will have detailed consultations with different stakeholders, in the hope that the ICANN community, all of you, will participate in that. We will do it probably through the possibility for written comments, written contributions, but hopefully we will have at least a virtual meeting, if not a physical one. But at least a virtual meeting to discuss the different comments received, and also that we can see and show how we will take these comments and some of the comments into account as we're finalizing the protocol.

JOANNA KULESZA: Thank you, Alex, most informative. It's my fault. I should have reserved 90 minutes for our conversation. Thank you. I promised the moments to Matthias. Matthias, any summary of this impressive exchange you guys managed to have?

MATTHIAS HUDOBNIK: Yeah. I want to thank you all for this very interesting discussion. Actually, I'm hoping we can tackle the question I was waiting at the end of my presentation. So I think you should be still open for new safeguards to implement, to tackle the domain name abuse related to end-users, but it needs to be realistic and also practical, as already pointed out in my presentation. We have still legal frameworks, we

have some criminal abuses which is very to the point to their country and where the criminal activity is happening. And otherwise, there are cooperative efforts like you have, and like I mentioned. Europol, for example, which is doing this under their remedies, but they are just coordinating and the legal basis are in the particular country where the abuse is happening. And the problem is, I think, to tackle exactly their country and also to still find maybe additional remedies. Nowadays with COVID, it's even getting worse. And I think it's very important that we find ways to have all the stakeholders involved so that we can find a [inaudible] proper solution. Thank you.

JOANNA KULESZA: Thank you, Matthias. Thank you. I think that's a perfect takeaway. We need to figure out where to feed this narrative. Thank you again, Alex, for joining us. I know you have a terribly busy schedule. Thank you for finding the time to explain to this community how the work that the Council of Europe has been doing for quite some time. You emphasized it could help us better protect end-user interest.

I'm going to stop here. I'm not doing a summary. Thanks to our wonderful panelists. Thank you, everyone, for taking the time to join us for the lively discussion in the chat. We will try to keep this discussion going in the context of DNS abuse, in the context of the Budapest Convention. We don't need to go beyond Budapest, as Alex clearly explained. Thank you to our staff. Thank you to the Tech Support team. Apologies to the translators for taking too long. And I

will just stop it here. The session is adjourned. Thank you, everyone, for participating.

ALEXANDER SEGER: Thank you. Bye-bye.

MATTHIAS HUDOBNIK: Thank you. Bye-bye.

MICHELLE DESMYTER: Thank you so much, everyone.

[END OF TRANSCRIPTION]