ICANN67 | Virtual Community Forum – One World - One Internet? Cybersecurity and Geopolitics in a Multistakeholder Environment
Wednesday, March 11, 2020 – 13:45 to 15:15 CUN

MICHELLE DESMYTER: Good morning, good afternoon, and good evening, everyone. This is Michelle Desmyter from At-Large staff. Welcome to the ICANN67 virtual meeting and the At-Large One World, One Internet Cybersecurity and Geopolitics in a Multi-Stakeholder Environment session on Wednesday, the 11th of March, 2020.

The Zoom room audio is in English. In order to access the French or Spanish audio, please join the French or Spanish streaming via the link on the main ICANN67 website.

All details were sent out on the ALAC Announce list with all relevant links. Details for these connections can also be found on the ICANN67 At-Large wiki agenda pages.

We will not be doing a roll call today for the sake of time, but ALAC members, RALO leadership, and liaisons, attendance will be noted.

If you would like to ask a question or make a comment in English, French, or Spanish, please type it in the chat by starting or ending your sentence with Question or Comment, and please keep them short if possible. French or Spanish questions will be translated into English and read aloud by a remote participation manager. First name plus last name. Staff will put periodic reminders of this process in the Zoom room chat. If you're in the Zoom room and you wish to speak, you may also raise your hand, and staff will manage the queue.

A friendly reminder to please state your name when you speak, not only for the transcription purposes but also for the interpreters to identify you on the audio streaming.

Finally, this session, like all other ICANN activities, is governed by the ICANN expected standards of behavior. I will go ahead and put a link in the chat momentarily to those standards for your reference.

Without further ado, I will hand the floor over to Joanna Kulesza. Please begin, Joanna.

JOANNA KULESZA: Thank you very much, Michelle. Thank you to all our panelists. Thank you to all our participants. We, the At-Large and the ALAC, are very much looking forward to this session. We look at this as an exercise in capacity-building and consensus-building. I'm really happy we have managed to welcome a diverse panel of speakers.

Let me start with a brief introduction, and then I will take us through the agenda we have formulated towards our speakers and the audience and a set of specific questions we would like to address.

Before I move on with the agenda, however, please let me note, as already said, that this is an exercise in capacity-building and consensus-keeping. What we are trying to address is a contemporary narrative for the One World, One Internet theme that accompanies

ICANN and its community. So what we are looking for is a comprehensive, across-the-community narrative that will help us to better communicate the work that is done within ICANN and that impacts the world outside.

Speaking of the world outside, we will try to look at the current, ongoing geopolitical events, themes, and issues that are being discussed in diverse fora.

With that, I welcome Leon Sanchez, the ICANN Board Vice-Chair. I am very much looking forward to Leon indicating the direction in which the Board wishes to lead the policy narrative when it comes to geopolitics. It is the first time, I believe, in ICANN history where geopolitics is explicitly mentioned in the short-term plans. With that, I welcome Leon and an intervention on ICANN and geopolitics.

I'm also very excited to hear a relatively brief recap of a very interesting paper that Veni Markovski with ICANN Org, the V.P. for U.N Engagement, published just a few days ago. You will find the link in our agenda. I strongly encourage you to read the paper either right now, because it's not very long, or directly after this session. Veni will provide us with a brief recap thereof, and we will try to see whether ICANN has a place/should hold a place in the ongoing geopolitical dialogue on cybersecurity and cybercrime.

We have Milton Mueller representing NCUC, who has done a lot of research and produced tremendous work—publications, papers, presentations—that refer to what is called Splinternet, or the process of fragmenting the Internet. Milton will present a few slides on state sovereignty. We're very much looking forward to that presentation. I believe it will provide us with a research background to the policy work that we're trying to discuss.

Last but not least, I'm really excited to have Patrik Faltstrom on the panel. It's actually Patrik and a few conversations we've had who've made me realize that this panel, this exercise, might be worth our effort and our time, even if it is done remotely.

Thank you, everyone, for joining us in this virtual ICANN meeting room. I'm very much looking forward to Patrik trying to frame the narrative from the technical perspective. That is the picket fence that ICANN works within.

I have reserved just 15 minutes for Q&A. In terms of housekeeping, please let me note we are very happy to have Milton Mueller with us, but I understand that he has another appointment. With that, I will provide for a short Q&A session right after this intervention devoted to that specific presentation. Then we will hear from Patrik, and then we will go to the Q&A session as scheduled. Those of you who know me know I'm a clock watcher, so I will do my best to keep us on time to stick to the agenda.

Having said that, as already indicated by Michelle, our wonderful staff will be keeping a watchful eye on the chatroom. All the questions posted in the chatroom will be then presented in the Q&A session.

If we could move on to the next slide, I will try to lead us into a discussion and try to identify what are the topics that we would actually like to discuss and to hear back from you because I know that we have participants coming from various communities. I'm also hoping we have representatives from outside the ICANN community joining us here today to discuss cybersecurity and cybercrime.

If we could move to the next slide, please, that would be wonderful. We will start off with discussing Internet fragmentation. I understand that Milton will be focusing on that specific term. But that is our point of departure. I am certain that none of the participants of this session missed the headlines that indicated that forever more states are looking to exercise their sovereignty online, and this is to be done by making sure that their section of the Internet remains safe. Working within the ICANN environment, we know that the Internet is [always] one network that we want to keep safe and secure. Those two narratives don't seem to be very compatible. So that's our point of departure. We want to seek answers to the questions on whether fragmentation is possible. Should it be possible, and how to deep into the layers of the network would it go? Is it just the content layer? Is it possible to have fragmentation below the content layer?

We, the At-Large, have been advocating for a shared narrative, for a better understanding, of DNS abuse, and we will use that reference also during this session. When we talk about DNS abuse outside the ICANN bubble, we talk about cybercrime and cybersecurity. I've heard this mentioned also during ICANN meetings: those two narratives should go hand-in-hand. That is also one of our purposes, one of our aims. We would love to find a shared narrative that brings the inside-ICANN narrative on DNS abuse and the outside-ICANN discussion about cybercrime and cybersecurity to a lowest common denominator. I'm wondering if that is an option we could explore, if there is a good answer to the question of a common ground between DNS abuse, cybercrime, and cybersecurity. You have a few of those topics mentioned here.

Yesterday, the At-Large hosted a DoH/DoT webinar or policy session, wonderfully hosted by Holly. We had the opportunity to learn a little more about DoH/DoT. We learned a little bit about The Simpsons, but we learned more about how to try and manage local networks. I would like us to link to that discussion. This is also why I'm really happy to have Patrik joining us.

As already indicated, I'm looking forward to Veni giving us more insights on the current work of the U.N. GGE and the Open-Ended Working Group. The report, should you read it—the brief report that Veni will be presenting—indicates ICANN's involvement with both of those panels. I would love to hear more about the relationship between that involvement, those platforms, and our GAC. Please let me note we have extended an invitation to GAC members. Unfortunately, no individual GAC member agreed to speak on this panel. I'm hoping they will join us remotely and also participate in the Q&A session. In that context, I'm wondering if there's a common ground to be found between the work done by the GAC, within the

GAC, and the governmental dialogue that's going on within the U.N. I noted in the report that Veni produced that ICANN has already had certain capacity-building sessions with diplomats. I would love to hear more about how that is going on and whether there's a chance for the community next to ICANN Org to participate in that process in a coordinated manner.

That brings us to Question #6: What is our role as the community in trying to keep the Internet as an entire one, safe, secure, and available network?

That brings me to the last question that you will see here on the slide but that provides a smooth transfer to our first speaker. The Board is well-aware of all of these issues going on. They have planned for the community and the Board to start this discussion within the next five years.

Without further ado, I welcome Leon. That's exactly my question: Which path are we going to pursue in trying to face those geopolitical challenges? Thank you so much. The floor is yours, Leon.

LEON SANCHEZ: Thank you very much, Joanna. Thank you for inviting me. Thank you for having me on this session. I think this is a very important topic to discuss.

To give a little bit of background on a possible answer, because I don't believe that as an individual or we as a Board have an absolute answer to the questions that are being posted, and, as you have rightly said, you might have noticed that, in the five-year strategic plan, we have a strategic objective which is highlighted as: Address geopolitical issues affecting ICANN's mission to ensure a single, globally-interoperable Internet.

So we believe that geopolitical and technical risks threaten the interoperability of a single Internet. Governmental policies, like the so-called cyber[inaudible] strategies, have already affected some of these Internet operations. One of these examples could be GDPR. You might be familiar with that acronym already. We believe that this and other initiatives could harm the way that the Internet actually works. To a certain extent, we believe that it could have such an impact that things wouldn't be the same if some of these policies were to be implemented and to become a reality.

To achieve these strategic objectives of addressing the geopolitical issues that could impact ICANN's mission, we have set also two strategic goals. The first one is to identify and address global challenges and opportunities within ICANN's remit by further developing early-warning systems, such as ICANN Org's legislative and regulatory development reports. If you see this strategic goal, we are talking about the continuous effort of identifying and trying to address these global challenges and opportunities. We are talking within the narrow remit of ICANN's mission. So it's not an effort that intends to overview the whole Internet governance ecosystem or the whole

Internet governance trends but only the very narrow scope if ICANN's mission.

In that fashion, we have established some targeted outcomes, one of them being ICANN org to continue developing and maturing systems to detect and monitor legislative initiatives and other governmental or intergovernmental actions or initiatives that could impact ICANN's mission or operations.

To this end, I believe that your question on what is the role of individual ICANN stakeholder groups in the ongoing global debates [of cleaning up] the network and, of course, following up on these trends is of the essence. We are aware that we are not alone in this, that we are not isolated in this, and we very much rely on the input and the work from our very diverse volunteer network and community to try to identify these challenges and these trends. So, if you ask me, I believe the answer for "What is the role of individual ICANN stakeholder groups?" is key for the community and the organization on achieving these goals and these objectives. Again, we need to work together as a Board, community, and organization to identify these challenges and to try to contribute in constructive ways to find solutions or at least common grounds and common lines of action.

Another targeted outcome is that ICANN Org proactively engages with the community to develop common awareness of ICANN's contribution to early-warning systems. This is a way in which, again, together, we can contribute to educate those who need to be educated. I'm not referring to any group in particular. Many of the efforts that we are trying to foster and to push for here are to be able to engage with those decision makers in order for them to have a wider perspective of the possible impacts and the possible unintended consequences that establishing regulations that are not mindful of how the Internet works and how the different layers interact could actually produce the adverse effects on technical issues.

Another targeted outcome is that ICANN has effective processes in place to receive and act on input from the community. This is something that we need to continue developing. You might be aware that we had the Internet Governance Cross-Community Working Group, which was transformed into an engagement group. I think that the work of this engagement group and this [inaudible] are essential to this targeted outcome. The more we are able to interact and feed each other with information and, of course, with strategies, I think the more effective we will be become.

Another targeted outcome is ICANN effectively convenes and facilitates discussion with relevant parties to help address relevant global challenges and opportunities. Again, to this end, I believe that closed communication and engagement with the wider community, the Board, and Org will be of essence to achieve this goal.

We also have identified some strategic risks like ICANN's inability to establish itself as a key player in the Internet governance [results and increase external] interventions by nation states or other entities and also failure to anticipate legislative efforts that force ICANN into a reactive mode. This is where, again, your role as individual stakeholders is of greater value to this effort. If we together are able to identify, follow, and address these challenges, then we will increase our chances, of course, of being successful.

The second strategic goal is to continue to build alliances in the Internet ecosystem and [inaudible] to raise awareness and engage with global stakeholders about ICANN's mission and policymaking.

It might come as a surprise, but not everyone knows what ICANN is or what ICANN does. So to build these alliances and to raise the awareness of how we do things, which kind of things we do, etc., etc., we believe will contribute to mitigate the risks and will help address the challenges of this geopolitical circumstances.

We also have established some targeted outcomes that identify some strategic risks to this end. To that, one of the targeted outcomes is that ICANN fosters successful and mutually beneficial relationships with local, regional, and global partners to ensure that knowledge-building about ICANN and its mission continues. Again, to this end, our community is our main strength. If we can build these alliances by collaborating closely with Org and with the different parts of the community, [inaudible] the world, we believe this could have a very important impact.

Also, we want to see that ICANN is engaged, its role acknowledged, and its present values in the arenas or topics within its remits discussed. So we want ICANN to be a trusted player and recognized player in this area. For these, again, collaboration across the community is pretty important.

Also, we want to see ICANN playing an important role in raising awareness of legislators, regulators, and stakeholders about its mission and the effect of various regulatory and other proposals on the Internet ecosystem.

I think one of the benefits that we have in this strategic plan is that we see this as a living document. It is not a document that was designed or built to rest in a drawer and be forgotten. We have been discussing how to keep this document alive and how to update it from time to time, not just for the sake of updating it and saying that we have new trends identified but actually doing this exercise of making sure that the strategic plan and, of course, the objectives and their goals are still up-to-date and up to the challenges that we might be facing at a certain point in time.

We have, as well, as I said, identified some strategic risks in relation to building alliances. One of them is the lack of understanding of ICANN's remit as it interferes with ICANN's ability to participate in relevant arenas. Again, if we don't convey ICANN's mission and its remit clearly, then we risk, of course, having misunderstandings on the scope of ICANN's work.

Another risk is that the Internet infrastructure, security, and government control continue to [vary] by region or nation. Again, to this end, our work with the community is of the essence. We don't know everything, but we have a very rich and diverse network of partners in our community that could help us sort these challenges and work together to overcome them.

Also, the [inaudible] single, interoperable Internet, such as alternative DNS roots or diminished commonality within networks [field doubt] in ICANN's ability to serve a global Internet.

So, as you may see, this is the vision of the Board in regard to this strategic objective. I believe, again, I don't have all the answers to the questions that you have posed, but certainly Questions 6, 7, and 3, I guess, are very important to the discussion when it comes to addressing the geopolitical issues that could impact ICANN's mission. So, on this, I would definitely encourage us all to continue working together to continue raising the issues that we see emerging, to continue the discussion rolling, and, of course, to continue discussing constructively as to the best ways to achieve addressing successful these geopolitical issues. We are sometimes faced with frustration and difficulties of not having all the tools that w may need to try to make our points in this arena. For this, again, our community is key, and I see it as our biggest strength in this all.

With this, Joanna, I would like to thank you. Of course, I'm happy to get further comments or any questions you may have. Thank you.

JOANNA KULESZA: Thank you very much, Leon. Thank you for staying and providing a timeframe.

I see a very lively chat, which is wonderful for any moderator. I see already people fighting in the chat. Brilliant. Thank you so much.

I see a hand up. Please let me exercise my authority as the moderator. I will keep all the questions to the Q&A section of this panel, as I would like to hear from our panelists first.

As you could by Leon's intervention, it was very comprehensive. There was a lot of controversial issues at times when it comes to regional or national legal acts that impact the network. As much as I feel tempted, I will not comment on these or ask my specific questions but, for the sake of time, I will just try to lead us into Veni's presentation, which I think will provide us with the context of what Leon was saying, emphasizing that ICANN tries to engage with other stakeholders and tries to raise awareness of the work that is going on elsewhere.

Veni's paper focused on the processes within the U.N.. I think it's a wonderful point of departure for further discussions. The overall questions is, is there any work for ICANN within the U.N. processes? One of those groups is the Open-Ended Working Group. Can we participate? Can ICANN Org participates? You will find some of these answers in the paper. I'm certain Veni will address them as well.

I'm curious, also—that is not in the paper—as to why do we have two processes? What was the genesis of those two working groups? Couldn't we just work together?

With that very provocative question, I'm going to hand the floor over to Veni. Thank you so much for joining us, Veni. The floor is yours.

LEON SANCHEZ: Joanna, please, may I interrupt? Just before we go to Veni, there's questions by Jim Prendergast in the chat, and I think that Goran would like to comment on it. So, if you don't mind, I would like to ask Goran if we could answers Jim's questions and then go back to the normal schedule

JOANNA KULESZA: Perfect. Let's do that. Thank you for the heads up, Leon. Goran, the floor is yours.

GORAN MARBY: Thank you. Can you hear me?

JOANNA KULESZA: Yes, we can, sir. Go ahead.

GORAN MARBY: Thank you. This is an answer back to Jim. First of all, it wasn't a year ago when I brought the idea of using this group as an interface between our interactions with the government to have a point in the community we can and talk about it on a more regular basis.

We have presented the idea to the SO and AC leaders, who I think are bringing it back to their respective communities. It's really not up to us to make that decision. It's really up to the community to make that decision. I think we all agree that it'd be good to have a regular interface between the work we do on the governmental [space] and the community so we can exchange ideas in a better way.

So the real answer to the question, Jim, is it's really up to you guys. We [inaudible] your proposal.

In the meantime, what we started to do is to give an—Veni can talk about that because he actually produced the first one—update and information paper on what we are doing and what we are seeing in different political venues around the world. The first one was from the U.N.. I know there's one coming out from the Brussels perspective, etc., etc.

On top of that, we also, in coordination with the stakeholders in India, we did, which is published on our correspondence page, have some technical views on the potential of a new legislation in India.

So we are doing things, but I agree with Jim. I would be nice if we formalized at least one place where we can come back to the community to discuss those things in a more orderly fashion.

JOANNA KULESZA: Thank you very much, Goran. With that, I hand the floor over to Veni, who am certain, on one hand, will fill that overall intervention with details. On the other hand, I'm just clock watcher here, so I'm certain we're good for time. Veni, the floor is yours within the appointed 15 minutes. Thank you.

VENI MARKOVSKI: Thanks. I have to tell you that this is such a lovely session. Leon actually mentioned some of the things that I was planning to share with you guys. Especially important, though—I want to stress again—is the fact the At-Large community is all over the world and has the insight and the understanding of what's happening nationally and regionally and sometimes maybe even globally that might touch on ICANN's remit. So my appeal to you is, when you see something, do let us know if it's national legislation or some kind of regulation or maybe a policy discussion that you think may touch on the single, interoperable Internet. That may come at some point to the U.N.

You mentioned the paper several times. While I don't expect people have read it, if they have seen it right now in the chat, they will have time to read it. It's a historic background on what ICANN has been doing at the U.N. with some updates about the latest discussions with regards to cybersecurity and cybercrime that are taking place at the U.N. We tried to particularly stress on the fact of things that actually mention either ICANN directly or indirectly. Yes, there are instances in which governments talk about ICANN, and they sometimes talk about what ICANN does. We do pay attention.

What we do … I want to make sure that there's an understanding that the U.N. is very different from the work that we do with the GAC. The GAC people are from the telecom administrations, mainly. Very rarely there would be somebody from a foreign ministry. I remember a couple of cases in the past few years where there has been somebody from a foreign ministry. That's why we need to do what's explained in the paper as well: a lot of briefings and outreach efforts—I call them educational outreach—in which we don't lobby for ICANN. We don't talk about necessarily the work that ICANN does, although we do that. But we also talk about how the Internet sanctions and what [inaudible] our organization there.

So the diplomats at the U.N. and the [inaudible] representatives who are covering the cybersecurity, cybercrime, and also [ICT] for development are very different committees at the U.N. General Assembly that covers those issues. We tried to bring all the factual information to them and make sure that they know, if they have a question, they can always ask us. If we don't know the answer, we also have the huge resources of people from the broader ICANN community who we can ask for help.

Now, I'm not sure who asked the question about whether they could participate in these discussions and this briefings, but these discussions are taking place at the U.N. and they are not open to the public. The only way for participation would be if somebody has access to the U.N. or somebody has ways of talking to the capital getting someone from the delegations to come to some of the meetings that take place at the U.N..

Now, this is the general thing about the work at the U.N. More concrete, with regards to that paper—I think, Joanna, you said there are three parallel groups that are working right now at the U.N.—we will find some new abbreviation. There is the Open-Ended Working

Group, the OEWG. Then there is the GGE (Group of Governmental Experts). Then there is a third group, the abbreviation of which is OECE (Open-Ended Committee of Experts).

The first group, the OEWG, is open for all the member states of the U.N. The GGE is open only for 25 member states. They actually send their experts there. The last group is the one that is going to work on a new cybercrime convention, and it's going to have its first meeting in August this year. So we are still looking to see what exactly will come out of this.

The OEWG already had two sessions—one last year and one this past February. A lot of views were expressed by different member states. It also had an open consultation—open but still within the framework of the U.N.. There were more than a hundred different organizations that showed up to express what their views are about cybersecurity.

What we do is really follow what's happening there and make sure that, if somebody talks about ICANN, what they say is factually correct. If it's not, we can correct the record. We try to really bring a lot of knowledge to these discussions from a neutral point of view from a technical organization in terms of very small segment of the unique identifier system. I think the paper speaks for itself. It's good we managed to publish it before the ICANN meeting [inaudible] so that you guys can read it and have questions. If you have any questions, let me know. I don't know, Joanna, if I answered all the questions that you asked in the beginning. I might have missed some. So if you don't mind repeating them.

JOANNA KULESZA: Thank you very much, Veni. I think there are more questions to be asked. The overall question, however, is how we could help. You indicated rightfully that those groups are not open to the public. My overall narrative here is that we might want to have a shared narrative within the community. We might want to take [this to] the outside. You indicated that the GAC might not be the best place/community for developing that narrative. So, in that sense, looking from the end user perspective, what is our interest in having this coherent narrative, and what could we as the ICANN community do to support this. Because you indicated that the work that you do on the ground is providing factual background to the discussions going on. Is there anything we could do to develop a shared narrative to take the word outside the ICANN bubble and support having One World, One Internet? Thank you.

VENI MARKOVSKI: Thanks. Just one correction. The GAC actually is quite relevant. What I said is that the GAC members actually do know what ICANN does. So we don't need to educate that much the GAC about what we do, though we do compared to the people who are from foreign ministries. So do capacity-building both for the GAC but also we do outreach efforts to the diplomats.

The way to help would be to reach out the capitols and talk to the people at the foreign ministries who are covering the United Nations.

Again, this has to be focused because you can't just reach out to any person at the foreign ministry. They have a huge amount of issues to cover. So the people can find out who is exactly in charge of the U.N. and other intergovernmental organizations and then talk to them and find out whether they follow these processes.

Now, to give you some insights on [inaudible], the bigger countries have bigger missions, but the smaller countries and mid-sized countries have smaller missions. So sometimes the diplomats will cover not one committee of the U.N. General, frankly, but two. When these two committees have competing sessions at the same time, obviously they are not able to go to both. So they have to choose where to go. If the discussion is not considered important enough, they may not show up. This could be at some point the discussions on cyber. If, let's say, parallel to cyber, there is a discussion at the U.N. Security Council about war and peace, obviously that's more important. Or, if something is related to health. It happened in the last few months.

So I think the way really to do it is—that's why I asked at the beginning—to reach out to the capitols, to the foreign ministries, to keep them informed and also to find out who from those countries is actually involved and interested in the discussions that are taking place at the U.N. and other intergovernmental organizations.

JOANNA KULESZA: Thank you, Veni. That is most helpful. I think we can stop here. I'm looking forward to the questions. I know we already have some in the chat.

With that, I would like us to move on to Milton. I know Milton has a presentation. Let's listen to that presentation and look at the slides. We will then allow for three to five minutes of discussion on that specific presentation, keeping in mind that Milton has another appointment later on. Then we will swiftly move on to Patrik.

Milton, the floor is yours. Thank you so much.

MILTON MUELLER: Thank you, Joanna. This is a very interesting central question, and I'm glad you put it together. I take it I need to cue the operator to change the slides. The theme of this paper is based on a book I wrote. My point here is not so much to advertise the book but to make it clear that there are far more well-developed ideas there that, if you're interested in this topic, I would recommend that you follow up on.

Next slide. The origins of my thinking about this came about three or four years ago when there was a debate—a post-Snowden debate—about the fragmentation of the Internet. What prompted me to explore this area was that it became very clear that there was no coherent definition of what people meant by fragmentation. In fact, it was more of a scare term that one side in a debate threw at another.

Here's a list of all the different thing that are sometimes called fragmentation by people in different contexts. Let's just take a bit of time to evaluate those. For example, if somebody cuts a cable outside by home by accident because they're digging, is that a fragmentation of the Internet? Suddenly my home is disconnected or maybe seven or eight different home are disconnected. I don't think we want to call that a fragmentation of the Internet. It's simply a temporary interruption in service for a localized place.

But what about data localization? Many of the charges of Internet fragmentation came about because of data localization laws. While I happen to think data localization laws are a very bad idea, it doesn't make any sense to call that fragmentation of the Internet. In fact, the data that is localized is typically fully available. It just has to be stored within a particular jurisdiction.

I have heard content-blocking referred to as fragmentation. We'll get to that later. I've even heard people say that paywalls could be classified as a form of fragmentation because they block some people's access to the Internet. But, if a paywall is an instance of fragmentation, then we're in trouble because many services on the Internet, including, in some sense, your Internet service provider, rely on you paying them to be able to offer a service.

National internets is another thing that's called fragmentation. I would just point out—there's a deeper analysis of this in the book—that most of the things we're calling national internets are not actually cut off internationally. They are highly regulated. They may be censored. They may be restricted in certain ways. But none of them are refusing to connect the global Internet. The closest you could come to an example of that might be North Korea.

Then there's some even sillier concepts of fragmentation. For example, I've heard some people say that language differences are an example of fragmentation. Well, that's not Internet fragmentation. That might be some kind of cultural fragmentation, but it's not a product of fragmentation of the Internet.

Next slide, please. So what is this debate about? Why are we talking about the fragmentation of the Internet? I tried to come up with a better word for what's really happening, and I want to call that alignment.

Alignment is talking about the—next slide, please—the mismatch between territorial boundaries of governments and the global connectivity of the Internet. So alignment is a process by which national governments attempt to assert sovereignty over a non-territorial cyberspace. It is really the driving force behind what most people are worried about when they talk about fragmentation.

Let's go to the next slide for a definition of what I call alignment. You see the nice man there trying to pound a round peg into a square hole. Alignment is the subjugation of the cyber-domain, which is non-territorial, to political jurisdictions, which are in fact territorial.

Next slide, please. We see here a list of three different methods of alignment. One of them is to declare the cyber-domain as a military matter—a matter of national security. We saw a lot of this happening in the United States, as well as Russia, China, and other major cyber-powers. We see the nationalization and centralization of threat intelligence and incident response. We see in some cases a move towards national technical standards, which could indeed eventually lead to true fragmentation of the Internet. We see kill switches in which you literally shut down the Internet or parts of the Internet in response to what is deemed a national security threat.

Another method of alignment is territorialization of information flows. That is when you, for example, institute content filters at the national boundary, where you engage in data localization, and where you engage in geo-blocking.

Finally, and fortunately for—and then most relevant to ICANN—is the attempt to engage in some kind of an alignment in critical Internet resources. By that, I mean names and addresses primarily. You have probably heard about some efforts to create national domain name roots. There was a proposal in the IETF by the Chinese to do that. And you've probably heard about national Internet registries, with which the national government tries to set itself up as the source of IP address numbers. But, for reasons I may have time to explain later, critical Internet resources were born global. They were established as part of global technical standards, and they took root in transnational institutions, such as ICANN and regional Internet address registries. Therefore, this part of alignment is extremely difficult and probably will never happen.

Next slide, please. I'm going to skip that slide. I think I've explained how cybersecurity gets … So what are the constraints on alignment? There are three of them that I have identified here. One of them is simply the global scope of the Internet that we've had for 25 years, really, [which] created a fait accompli in which names and numbers are globalized in terms of their administration. We set up a global institution called the Internet Corporation for Assigned Names and Names to globalize the governance of the domain name system. We have the default interoperability of [the Layer] 3 and 4 Internet protocols such that it creates this global compatibility. So, if you want to interfere with that, you have to do the work rather than the other way around, like with a telephone system, where the national system has to agree to interconnect internationally.

Another constraint is economic efficiency. We all probably know about the network externality, which means that certain economic goods become more valuable as more people use them, and certainly the Internet is benefiting for that. We would be sacrificing share in economy, and we would be sacrificing competition and innovation if we withdraw from this global compatibility.

Finally there's what I call the jurisdictional paradox, and that is, when a territorial government tries to assert control over the Internet on a territorial basis, it really has to choose between that control being very limited and ineffective or trying to globalize that control.

Now, I have here the U.S. versus Microsoft case, but I think perhaps an easier and better example in this context is the idea of the right to be forgotten, where, let’s say, the French government wants to enforce the right to be forgotten on Google in its own jurisdiction but it finds that it can’t really make that right effective in France only. So then we have the European court declaring that Google has to implement this right to be forgotten globally. Of course, that’s a paradox because, in some countries, notably the United States, there is no right to be forgotten. So you end up with one state, in effect, globalizing its jurisdiction at the expense of other states, which is one of the reasons why I believe the sovereignty is simply incompatible with the Internet.

Let’s go to the next slide. Here’s where I get radical—unashamedly radical here. I mean, somebody has to say this, and that is that fundamentally there is a contradiction. We can try to pretend that this can be resolved and there may be middle grounds that we can find over a long period of time. But, fundamentally, cyberspace is global, and governments are territorial. The way to solve that governance problem is that we have to come up with some notion of popular sovereignty in cyberspace. That is, cyberspace has to become self-governing, somewhat independent—not entirely independent but somewhat detached—from the territorial jurisdiction of nation states.

Next slide. Some of you, if you think that I’m crazy or that I’m speaking to something that’s impossible, I hold before you my Exhibit A of something where we actually did fight for and achieve popular sovereignty or self-governance in cyberspace in a way that’s directly relevant to ICANN, and that of course is the IANA transition.

Now, for those of you who are not in the United State, you may not be aware of the degree to which the IANA transition raised fundamental questions about the relationship between national governments and the global governance of the DNS. Some of you may know that some rightwing or nationalistic legislators were opposing the Obama administration's attempt to do the transition by claiming that the U.S. was giving way the Internet to Russia and China. So the assumption behind that assertion was that some nation states got to be in control of the Internet and it should be us and not Russia and China. But, of course, the actual position of the transition, if you recall, was that control should rest in the hands of what was called the global Internet community. That is, we should be working for self-governance in cyberspace and not national governance.

Next slide. Let me just give you a few more examples of how this is directly relevant to ICANN. First of all, ICANN's status … We created ICANN specifically to avoid jurisdictional fragmentation, or rather alignment, of DNS with nation states. That's why we have ICANN. We keep refighting this battle. We have to stand up for this capability of ICANN to be a globalized governance entity.

Another example of how this is coming up again is with the controversies over WHOIS in making it compliant with the GDPR. There are people who are saying, "Well, let's make WHOIS conform to GDPR but only in European jurisdictions (or only in specific jurisdictions). If the user and the registrar are outside of those jurisdictions, let's have a different set of rules apply." So some people are even talking about fragmenting authority within the context of ICANN governance. I think we really have to understand that the whole model that we're working with here is based on a non-sovereign, integrated approach to cyberspace governance.

How am I doing for time, Joanna?

JOANNA KULESZA: You are doing wonderfully well for time. Thank you so much for being beautifully provocative. Thank you for that. We have now more than three, but we have three questions in the chatroom. I would hand over to our staff to read them out to you. Maybe you could link to the questions and whatever other facts and lovely provocative statements you have at hand. Would this work?

MILTON MUELLER: That sounds good.

JOANNA KULESZA: Perfect. Thank you. So I'm going to hand it over to Evin and kindly ask her to read out the three first questions we noted for you for this presentation specifically in the chat. We will then move on to Patrik, making sure he has the promised 15 minutes, and then we will move on to the Q&A, should you find the time to keep joining us. Evin?

EVIN ERDOGDU: Thank you so much, Joanna. I'll read off the first question from Zakir to Milton. He says, "How about alternative roots fragmentation? And [the] recent test by Russia--#areyounetfragmentation. Thank you."

JOANNA KULESZA: Evin, if we could go with the three questions first and then have Milton answer all of those. Thank you.

EVIN ERDOGDU: Yes. Can you hear me okay?

JOANNA KULESZA: Yes. Please go ahead.

EVIN ERDOGDU: Sure. The second question is from Javier Rua-Jovet. He says, "Question to anyone that will take it. I see quite a lot of ALAC collaboration with the GAC. That is probably generally a good thing. We just had a good meeting with the GAC. Lots of joint postures and agreements. Actually, some ALAC members, including myself, have worked for governments in the past. So those conversations seem natural and easy. But what are the dangers, if any, of the ALAC/GAC closeness when it comes to ICANN geopolitics—specifically the central issue of keeping DNS and IP governance under the sovereignty of we the people of the Internet and not under the power of governments, especially non-liberal ones, for the [IG]? And shouldn't the ALAC, which stands for individuals, not governments, always be at the front lines of the defense of the non-governmental model of IG?"

Our third question is from Imran Hossen. She says, "I'm new at this type of meeting at ICANN. I do not have any idea about IX policy. So I have a question about IX. There's many IX developing from private organizations and community, like BDIX, Equinix, and more. I see those IX are going to popular and business community and users. I need to know, is there any regulation or control or policy from ICANN for those IX. If there's no control on those IX, I think there is a threat to the Internet. If there is no policy for IX, what do you think about this? Thank you."

So those are the three questions. I'll turn it back over to you.

JOANNA KULESZA: Thank you so much. I'm going to hand the floor to Milton. To the best you can answer those, please try to do so. We will move on and come back to the questions in the Q&A session. Thank you.

MILTON MUELLER: All right. I will address the question of alternate roots and Russia first. The question of alternate roots is one which is a good example of how the value and cohesiveness of the Internet relies on the network externality. Anybody can form an alternate root, but, because any such alternate root is likely to lead to incompatibility in naming, very few people are going to want to use that root. Since the ICANN root maintains global compatibility through the choices of users and through the power of the network externality, it's very unlikely that anybody will ever establish an alternate root.

I have a couple of students working on the question of Russia and it's so-called alternate root. It's not an alternate insofar as Russia actually knows what it's doing with this new legislation. That is somewhat questionable because some of the legislators involved clearly do not understand what they're doing.

But, insofar as they're doing anything, they are creating a backup system that would protect them against the perceived threat, which is not a very real one but is perceived by some people in Russia, that their top-level domain or their domains would somehow be cut off from the Internet by action by the United States.

So, insofar as Russia is doing anything meaningful and interesting, it is simply that they are creating a backup system for DNS that would protect them from interference by the United States. At least that's the way I understand what they're doing.

I very much like this second question. Somebody is talking about the potential dangers of the At-Large and the Governmental Advisory Committee cooperating too closely. I think the fear in the question is that the ALAC would be coopted. I can see why the At-Large Advisory Committee has some kind of alliance within ICANN politics with the GAC because they [both] advisory committees, they both have no direct role in policymaking, and they are offering advice. So both of them sometimes feel like they need to be heard. So that's fine.

But I really like this question, which is, "Shouldn't ALAC be in the forefront of advocacy for popular sovereignty in cyberspace?" Yes, indeed it should be. Indeed, its origins were in fact a very radical experiment with individual voting to govern ICANN. It used to be that At-Large members were considered members of ICANN. Well, let's just say that certain elections had the wrong result, so the electorate was abolished. The At-Large was made into an advisory committee instead of a membership entity.

But, be that as it may, right now I do think that At-Large should be at the forefront in advocating for the empowerment of the people of the Internet—that is to say to the users and consumers and producers of the Internet—in Internet governance.

Finally, the IX, I assume, is Internet Exchanges. Insofar as I understood the question, it was about whether they are regulated by ICANN. Of course, I can see certain Board members and staff members of ICANN turning purple when asked that question. They will tell you emphatically, perhaps more emphatically than I will, that they do not regulate Internet exchanges. They handle the governance of domain names. Insofar as Internet exchanges use domain names, they are subject in some minimal sense to ICANN authority, but the operation of an Internet exchange is really not affected by anything ICANN does very much.

That's it from me. I hope to hear from Patrik now.

JOANNA KULESZA: Thank you very much, Milton. I have so many questions, but I'm going to refrain from asking any of these. Thank you for being so wonderfully provocative.

Patrik, right into your hands. Please give us the technical side of things. We already heard there is a need hear again about the DoH/DoT. We heard a little about the rationale turn of the roots and whether this is going to work or not. We have Andrei in the chat also commenting. Straight into your hands, sir. Help us figure this out. Thank you.

PATRIK FALTSTROM: Thank you very much. So this all means that I have to go back and redo my slides, I presume. I'm Patrik Faltstrom, the Technical Director and Head of Security at Netnod, which indeed do operate one of the larger exchange points in the world. So that was interesting questions regarding governance. I will come back to that.

Next slide, please. The first thing to remember is to look into what we actually mean by some kind of security problems. The first thing I would like everyone to remember is what to do when something is happening. When something is happening, you have some kind of event and you need to have a process for how you take care of that. in the global world, when we have so many different players, it's real important to also do this coordination globally, across organizations and sometimes, as Milton explained, across country boundaries.

Unfortunately, this is not something that governments have understood. As Milton explained, just because we have the mismatch between country and jurisdiction boundaries and organizational boundaries for whoever operates what they are providing—that is part of the Internet—that creates a challenge by itself. Many governments has imposed on organizations to run very formal process[es] for incidents and making sure that the Internet stays together, similar to this … This is my personal process that I'm using, but trying to do this in the society is really, really difficult.

Next slide, please. If we then look at what I mean by security issues, we talk about incidents, and there was some discussions about spam. I've been working with the Royal Academy of Engineering Sciences in Sweden that came up with that report. In that report, we draw the conclusion that none of the terms—information security, IT security, or cybersecurity—is defined.

In any discussion, when you hear someone talk about cybersecurity, ask them what they mean and see whether they can explain. The terminology that I will use here and what is used in the report by the Academy of Engineering Sciences is that information security is related to all information and all kinds of threats. IT security is any kind of threat and anything related to digitalization when information is digitized. When we talk about cybersecurity, which is what I work personally on, we talk about incidents that are related to antagonists when someone really wants something to happen.

So the question about spam I think is just completely wrong because spam might be a tool that is used for someone to reach some kind of goal. So already, when talking about spam and whether that is something right or wrong, I think the discussion is not really focused enough.

And, as Milton said regarding Russia legislators and also legislators in some other countries, including my own country, Sweden, sometimes they don't know how the Internet works and they legislate against the wrong kind of thing. I will explain that a little bit later.

Next slide, please. Another finding that we had that we concluded in the report is that we no longer have pipes. Historically in telecommunication, you had one player that was responsible for absolutely everything, from the cables through the services and everything. Today we have horizonal layers, so we have moved from having pipes to lasagna. In this lasagna, we have multiple layers. You have the IP layer. You have the TCP layer. You have the HTTP protocol. Then you have the DNS protocol. And you have various URLs and DNS and whatever it is. In each one of the layers in the technical architecture that we call the Internet architecture, you have an addressing. You have to look at one layer, each layer, one at a time.

Now, unfortunately, the market economy has interest in building pipes. That is why we see that the Facebook chat service is only provided by the Facebook company. And the same thing with many other kinds of services which are pipes. But the Internet architecture is actually horizontally-layered, and that's why we have all of the protocols that are layered on top of each other.

Next slide, please. One thing that has happened is that, to be able to have more security, we see more and more encryption going on on the Internet. What I mean by encryption is that, for each one of the layers that we saw in the lasagna, we try to apply as much security as possible. We need to encrypt the layer. We need to have digital signatures on the layers. Sometimes people use password technologies like blockchain to add some kind of security. This is from the [inaudible] report in 2019, so it's a little bit old. But you see that the amount of web traffic that is encrypted has increased. The number of messenger applications that are encrypted increased. Also, the Internet [inaudible] task force and everyone else and all of us. We want to have more security. We want to have a padlock. We want to have DNSSEC-signed domain names, and everything should be secure. But we have to remember that the security is supplied at one layer at a time.

Next slide, please. If I may take one example of this architecture, I simply things but saying we have three different layers here. At the bottom we have IP packets that are flowing in the network. It uses IP addresses from the sender and the receiver. Among all the IP packets, it's possible to identify, in the Internet architecture, packet flows. These packet flows uses 5-tuples, which consistent of the protocol, which is, for example, TCP or UDP. You have the sender and receiver port and IP address. So this ends up being a 5-tuple which identifies the communication that is happening over the Internet. Using these flows—one or many of them—have an application. The application itself could be, for example, a web browser connecting to one or many webservers to fetch the information and paint a webpage in a web browser. So we have these three different layers, and we have to look at each one of them and see what's happening.

Next slide, please. If it is the case that we are starting to encrypt communication—for example, with TLS in the HTTP—what we're doing is we're encrypting the top two, which is black. So whoever looks at the packets can no longer at what's inside the packets, what's flowing on this layer. But it can still look at the IP packets with the IP addresses and it can do the packet flow identification. But it cannot look at what's actually in the inside the flow itself, which means that the encryption makes it harder for whoever is looking at the traffic and trying to guess what's going on. It's much harder for that party because the entity only has the two lower layers in this lasagna with only three layers. That's the only data that they have to be able to make a judgement on what is going on here on the network. Of course, that is one of the goals with encryption.

Next slide, please. To go back to what Milton was talking about, we have two parties which are communicating. The green is communicating with the red. The green and red use two different ISPs in two different jurisdictions. You see the two different pipes there, one for DNS and one for HTTP, and you see that the DNS pipe is actually broken there. The DNS query is sent from the green to another ISP, which in turn [is sending] the DNS query over to [the Another] party that sends responses back. Then the green party is opening the question to the red to actually fetch the data. This is what it had looked like historically. We see that both ISPs had the ability to look both inside the pipes and between the pipes, and they have roles here.

Next slide, please. The first thing that we did on the Internet was that we started to encrypt the HTTP traffic. By encrypting the HTTP traffic, it's impossible for another ISP in some other jurisdiction to see what's going on there. Indeed, it's also impossible for the one ISP in jurisdiction to see what's going on because the connection between the green and the red box is encrypted.

Next slide, please. What is now going on by adding encryption also to DNS is we see that, for example, by one way of deploying DNS-over-TLS, we have the DNS is a separate tool, but the connection between the green and another ISP is encrypted. So it's not possible to wiretap, for example, between the green box and the Another ISP. The rest of the connection is still the same. So both the Another ISP and One ISP is able to look at the traffic and do whatever they want to do with the traffic.

Next, please. Another thing that can happen is that people use DNS-over-HTTPS. What is then happening is that not only is the DNS traffic sent directly to a DNS server somewhere but also some deployments actually send the DNS traffic in the same tube, the same flow, as

HTTPS. It's also the case that the traffic goes all the way to a player maybe in some other jurisdiction. So, in this case, we have both HTTPS and DNS within the black tube, so it's impossible to actually look at what's going on. So neither One ISP nor Another ISP in either of the two jurisdictions is able to know what's going on here. The only thing that the two ISPs can do is to look at the flows that are used and also what IP addresses this traffic is sent between.

Next slide, please. So the interesting thing here is that you can, of course, talk about other examples. We heard the example of, for example, alternate roots, who's actually signing that, how do you validate things that are signed by entities that you don't trust, or what kind of risk is there that someone might lie to you. But the whole idea here, the whole problem—I completely agree with Milton, which is interesting because those who know me and Milton know we've had long discussions the last 5,000 years or so about these kind of things—is cross-border transactions. When you have conflicting rules in conflicting jurisdictions, which ultimately is because of conflict of use and norms in different cultures, how do you handle that? How do you handle when two different jurisdictions have competing laws?

When you have jurisdiction and when you have legislation, you ask someone to do something. You say that, according to that jurisdiction, someone is responsible to do something. Here we come to, for example, various court orders—for example, in Sweden—that have asked ISPs to block access to certain URLs, to certain webpages. The ISPs have sometimes implemented that by blocking DNS lookups for certain domain names. How can they do that when the DNS is encrypted? They can no longer do that.

So the question then is, of course, is it the correct thing to ask the ISP that cannot see the DNS lookups to block access to webpages? If that is the wrong question, who has that responsibility? None of the players? Well, if you have jurisdiction and a law that say access to that webpage is wrong, who is responsible to block that, and what tools are they requested to use? Who knows?

So the ultimate question is, who is responsible for what when you have cross-border transactions when you are applying DNSSEC security encryption and digital signatures, which are technical solutions that are designed to ensure that no one can touch the traffic? So, to some degree, this is a competition. That’s why it’s so important, just like Milton said, which I also completely agree with, that whoever is the legislator needs to understand the layers in the lasagna and needs to understand security measures you want to have so that no one can use someone else’s credit card. Given that you have a certain architecture, certain things are encrypted. Other things are signed. But you need to agree on who is actually responsible to do what. That is the only thing that you can implement in local jurisdictions. Hopefully, over time, we will see a greater harmonization in the legislation of various jurisdictions, and because that is, of course, what creates stress. But there is difference in the legislation in various jurisdictions. Thank you.

JOANNA KULESZA: That is perfect timing, Patrik. Thank you so much. Again, trying to be the moderator here and not overstep my role, according to the agenda, we will proceed as plan with that.

I see one hand up. I would like us to start with the questions in the chat. The chat has been wonderfully lively. Please let me note that this has been an exercise. We were trying to get a feel of the room on whether this topic would be of interest. It seems that it is. I would be more than thrilled to pick this up again, possibly during a face-to-face meeting, as I believe that would add to the conversation. We have Jonathan on the call as well, and I've seen folks indicating that this might be of interest to our Consolidated Policy Working Group.

I look at this as a capacity-building exercise. So this was more about informing the community on where we stand and what are the ideas that are popping up across the board.

With that, I would like to take three questions from the chat. I know Evin has been diligently taking them. Please, Evin, can you read out the questions? If they have been addressed to a particular speaker, please kindly indicate that speaker. I understand Milton has had to leave us going into another appointment. We have ten more minutes. We'll start off with the three questions. We will give our panelists a chance to respond. I will do my best to reserve three minutes for the one hand up that is there providing [SK Cyber] a chance to comment or to ask a chance that will be responded to off the record. Evin, over to you. Thank you so much.

EVIN ERDOGDU: Thank you, Joanna. We currently have two more questions and one comment. I'll read off the two questions first and then the comment. The first question is from Gangesh. He asks, "How far does the proposal for popular sovereignty align with the concept of global commons in international law or a common heritage principle? Do you see potential for framing it through these or similar principles under international law?"

The second question is from Andrei Kolesnikov. He asks, "Do you see the increase in IX traffic due to remote workers (COVID)?"

The final comment is from Javier Rua-Jovet. He says, "Some liberal states have threatened with building national Internets and alternative DNSs, but Professor Mueller has proven that the network benefits. The benefits of staying in the global Internet makes such threats ring quite hollow and have not happened. China wants you to buy its goods on eBay, and China knows eBay works because the DNS/IP system works."

Thank you, Joanna. Back over to you.

JOANNA KULESZA: Thank you, Evin. I see Patrik's hand up. I believe that is an attempt to answer our questions, so I'm going to give the floor back to Patrik. If Veni or Leon would like to comment, please kindly raise your hand. Thank you so much.

LEON SANCHEZ: Thank you very much. Yes, it's an attempt to answer at least part of the questions here about international law. I think international law is difficult. I would like to see more coordination between the legislators in the various jurisdictions. Lots of the legislation regarding the ability to build Internet in the world—for example, access to [dark fiber and others]—is hidden somewhere in the telecommunication legislation and not in the real international law.

I would like to see more countries, including, for example, Sweden, ratifying the Budapest Convention on Cybercrime, which makes it easier for law enforcement in countries to do MLATs and hand over information.

So I don't really know whether we should hang things and rely on international law. I think cooperation is important, regardless of how that is implemented.

Regarding IX, I think there are people that have seen an increase in traffic on IX and elsewhere on the Internet in the last couple of days. We should all be aware that there have been a couple of upgrades, specifically on gaming on consoles as well, specifically during the last 48 hours. So one should look at trends and a little bit a longer time before you draw conclusions. But we all see in social media that a lot of people do more remote working. So let's hope that the Internet sticks together.

Personally, I'm a little bit sad that people do not take the Internet for granted, just like they do with water and electricity. I think water, electricity, and the Internet should be as stable and as necessarily and as functional all over the world. This is specifically including water that we unfortunately don't have all over the world. But all three is needed.

Regarding a separate Internet, we already heard a couple examples. It's something like password technology, passwords also in the discussion—to be able to really dig into it. We need to talk more about what we really mean about it, just like [inaudible] talking about. So we need to talk more about that, specifically in the context of DNSSEC. Thank you.

JOANNA KULESZA: Thank you very much, Patrik. I'm wondering if Veni or Leon want to pick this up. Patrik mentioned legislative coordination. I believe that is something that the U.N. is doing very much. If any of our panelists would like to pick this up, I'm happy to give them the floor.

If that is not the case, I'm going to take the lonely hand that's been raised for quite a while. Thank you very much, [SK Cyber]. The floor is yours. Please feel free to ask a question or comment.

[SK CYBER]: Okay. Thanks for [passing] me and thanks for the nice presentation. I have a question here. I'm really concerned about technical standards, development cases, like there are necessarily for the standards, frameworks, and even the best practices in areas such as digital forensics and coordination in incident responses. These are the problems. Even Europol, Interpol, IT, and the United Nations all have their agendas as one of the priorities listed. So how are we going to address these issues through ICANN?

The second thing is, there are state-sponsored attacks which are being proven now. How can ICANN play an effective role against it, being aligned with the communities? And how we can educate and develop the capacity among the people?

These are my key concerns. Thank you.

JOANNA KULESZA: Thank you very much, sir. Are those targeted at any specific panelists?

[SK CYBER]: Any of them can answer. I'll be happy to an answer from any of them.

JOANNA KULESZA: Thank you very much, sir. Let me just recap. We're looking at digital forensics and attribution of cyberattacks and the role that ICANN holds in those. I know we have a few Board members and ICANN Org members here on the panel. If anyone would like to pick this up, I'm looking for hands raised.

It seems we do not have a specific answer for your question, sir—

PATRIK FALTSTROM: I can help a little bit.

JOANNA KULESZA: There you go.

PATRIK FALTSTROM: Let me add a comment there on why attribution is important for cyberattacks. In lots of the legislations that you have in many jurisdictions—Sweden is the one that I know, for example—if it is the case that you have some kind of attack that is happening on Swedish territory, if it is the case of the attribution of that attack—I'm not talking about cyber; I'm talking about if something is happening on Swedish soil—if that incident is created by another state, then it is a problem for the military defense to take care. If it is not another state doing it, it's a matter for the police. So attribution is something that unfortunately often is needed to be able to even know who's going to deal with a problem. This is, as I said, not something that is tied to cyber but also to other incidents.

So the question, I think, is very, very valid. I see a lot of academic work, including some that I participate in, that are looking at the issues with attribution. Thank you.

JOANNA KULESZA: Patrik, is that a concluded statement? It seems like we lost you.

PATRIK FALSTROM: Yes, that is concluded. I am done. Thank you very much.

JOANNA KULESZA: Thank you so much. All right. So that gives me three minutes to wrap this up. Please let me just note—I cannot refrain—there is a lot of work being done on attribution of cyberattacks.

I see Evin's hand, so I understand that would be housekeeping. Evin, please go ahead.

EVIN ERDOGDU: Sorry, Joanna. We actually have one more question, if time permitting. I could read off from Holly.

JOANNA KULESZA: Please, let's do that. Thank you.

EVIN ERDOGDU: Sure. Holly asks, "How should a national entity deal with the need to block content—or can it?—once DoH/DoT is in place? Thank you."

JOANNA KULESZA: Would Patrik like to pick this one up as well? Because that seems quite specific and technical.

PATRIK FALTSTROM: Yeah. I think we in SSAC had a session yesterday which went into the details of DoH and DoT. It's also the case that SSAC also tried to explain that there's a difference between the protocol itself and the deployment of the protocol.

So I think the important thing is that, with a different way of dealing with DNS, you might have different entities dealing with the DNS queries. So the question is whether the same tools can be used for blocking as before and whether the same entities can be responsible for doing the blocking and managing the blocking as before. There are big question marks there.

So I think the answer is that that needs to be reevaluated, which of course also means that some legislation needs to be reevaluated and some court cases need to be reevaluated. It's a hard question, a good question.

What I'm nervous about personally—this is definitely not an SSAC view—is that there is, today, a responsibility for the access providers that is often today running the local resolver; that they, by blocking certain domain names, are doing enough—some definition of enough—to block access to certain content, when instead the only real way for blocking content is to do proper takedowns. Thank you.

JOANNA KULESZA: I think that is a wonderful summary. I think this is what it's all about: the fine line between DNS abuse and the role that individual actors play as opposed to national policies.

We have one more minute for me to try to wrap this up Thank you so much. Thank you to our panelists. I'm convinced that the presentations have been most informative. I learned a lot, and I see from the chat that so have our participants. Thank you, everyone who participated. Thank you to our interpreters. Thank you to our staff and technical support. Thank you to everyone who has taken the time and those, at times, in awkward time zones to join Cancun time. As already said, I would be more than thrilled if this theme could picked up within At-Large or beyond. As we proceed, do feel free to get back to me with any comments that you guys might have. We're available for questions and comments.

Thank you so much. Enjoy the rest of your day or evening. Bye.

[END OF TRANSCRIPTION]