KOBE – At-Large Leadership Working Session: GCSC & GNSO Chair
Sunday, March 10, 2019 – 15:15 to 16:45 JST
ICANN64 | Kobe, Japan

OLIVIER CREPIN-LEBLOND: [inaudible] in cyberspace the GCSC members that are coming to meet with us and discuss all the work they've been doing in the past years?

LATHA REDDY: Two years.

OLIVIER CREPIN-LEBLOND: Two years. It goes really quickly. I remember when it started. We have new Co-Chairs, Michael Chertoff and Latha Reddy, who have taken over from Marina Kaljurand, who is still at the table.

So, welcome, everyone. It's really exciting for us to see you here. I'd like to thank Wolfgang Kleinwaechter for having suggested that we have such a meeting with the ALAC and over in an ICANN setting. I believe it's the first time you are in an ICANN setting for discussing your work. So it's really exciting to see the number of people around the room.

I'm not going to ramble on forever. I guess I can hand the floor over to Latha Reddy, who's going to be taking us through the work of the GCSC. Thank you.

LATHA REDDY: Thank you. Thank you very much, Olivier.

OLIVIER CREPIN-LEBLOND: Oh, and there is a housekeeping note, of course, which I need to go for. So, Gisella, please.

GISELLA GRUBER: Apologies to have interrupted. Gisella from staff. Just to remind everyone that this session has English, French, and Spanish interpretation, as you may be getting question in those languages. Unless you speak them, please do use your headsets. We have the interpretation booths behind us, so if I could kindly ask you to please state your name when you speak each time to be identified on the language channels and also for the transcript, and also to speak at a clear and reasonable pace to allow for accurate interpretation. Thank you very much.

LATHA REDDY: Thank you.

OLIVIER CREPIN-LEBLOND: Thank you, Gisella, and over to Latha Reddy.

LATHA REDDY: Thank you, Gisella, and thank you, Olivier, for inviting us to make this presentation. My name is Latha Reddy. I'm the Co-Chair of the Global Commission on the Stability of Cyberspace. Our mission is to engage the full range of stakeholders to develop proposals for norms and policies to enhance international security and stability and guide responsible state and non-state behavior in cyberspace.

As Olivier mentioned, we launched this commission two years ago at the Munich Security Conference. It's a joint initiative of the Netherlands government, the Hague Centre for Strategic Study, and the EastWest Institute. The latter two think tanks act as the Secretariat of the group.

We were three Chairs, with Marina as the Chair and Michael and myself as Co-Chairs. Consequent on Marina being elected as a member of Parliament in Estonia, she has stepped down as the Chair, as I believe the rules don't permit her to be the Chair. So Michael and I have taken on joint chairmanship of the commission.

We have 25 commissioners, [and] as was already mentioned, the Secretariat, and we are a multi-stakeholder group. We have Civil

Society industry and people with government experience, such as myself. I'm a retired diplomat. Michael is a former Secretary of Homeland Security from the United States. We have a research advisory group. We have a management board, and we have a government advisory board. So we have the whole bureaucracy.

I wanted to say that, as I mentioned briefly what our mission is, what we managed to achieve so far is to formulate and release eight norms into the public space, which we hope will reach the leaders, the policy makers, all over the world. We are also coordinating with many other bodies, including some of the U.N. agencies. Marina is also a member of the U.N. Secretary General's high-level panel on digital issues.

Basically, what we thought we'd do – because I think the norms themselves explain better than we can what kind of recommendations the commission is focusing and what our final report will also focus on. It gives you an idea what we believe is important to keep our cyberspace open, secure, and safe, and also not stifle innovation.

So we have eight norms, and the first one norm I'd like to ask one of my colleagues from the commission to present to you is the call to protect the public core of the Internet. I'd request Wolfgang Kleinwaechter to kindly request this norm. May I request my

colleagues to kindly keep the presentation to two minutes each so that we then have enough time for discussion?

WOLFGANG KLEINWAECHTER: Yes. When we started to discuss norms, the idea to have a special norm to protect the public core of the Internet immediately got full consensus among all members of the commission because, while on the one hand the stability of the public core is guaranteed by its design a distributed system, with the root servers, and SS servers – it's difficult ultimately to kill the Internet; there is no kill switch for the Internet as such, so that means you have a lot of elements in it which guarantees a certain stability – on the other hand what you have seen in recent months and years are ongoing attacks against the public core. Just recently, the DNS hijacking I think is a new dimension that could undermine the stability and security of the Internet.

So far, I think to have a special norm which would bring acuity to state and non-state actors not to touch the public core and to guarantee that this remains stable and to work together to find the criminals who do some bad things with the public core or plan to do things with the public core. It's extremely important.

We also had a discussion on whether the attack against the public core of the Internet would be a special category of, let's say, crime

or cybercrime, as you have in general a criminal law where you have crimes and then crimes against humanity because, if you would attack the public core, the Internet is so important for all activities of life today that, really, this could be a special category.

So these are still issues for the discussion, but our understanding of the public core of the Internet is very close to ICANN's mission because we see the public core of the Internet [as] the DNS, the routing system, and the numbering system.

So far, when we started a discussion – do we have something in common with ICANN (the global commission and ICANN)? – we discovered that work [inaudible] the protection of the public core of the Internet is one of the key elements where we have common interests. We are coming from different corners. ICANN comes more from a technical perspective, the Global Commission more from a political perspective. But there is an area for common interest.

We are also here to identify fields for further cooperation. We will have a meeting with the Security and Stability Advisory Committee later today. It would be also very good to get feedback from the users community, the At-Large community, on what they think should be politically done to protect the public core. Thank you.

LATHA LEDDY: Thank you, Wolfgang. I'd now ask Marietje Schaake to present the norm on the call to protect the electoral infrastructure.

MARIETJE SCHAAKE: Thank you very much. In my daily life, I'm a member of the European Parliament and I'm from the Netherlands. What we try to do with the norms that we work out is to also anchor them in international law principles where we can so that we're not reinventing the wheel but that we're really building on a body of agreed principles.

So the following norm is anchored in two international law principles. One is the norm of non-interference between nations. It's part of the U.N. charter and it's obviously key. The U.N. charter says that all member states shall refrain from threats or use of force against the territorial integrity or political independence of any state or in any manner inconsistent with the purpose of the U.N.

Now, when you read the universal declaration of human rights, you find there that the rights to elect on the basis of universal suffrage and secret ballots [of] one's government is also protected in the universal declaration.

Clearly, when you look at electoral processes, whether they be done with paper ballots or electronically, every election now has

digital and IT components. There's a lot of attention, on the one hand, in the public debates on this information, but we focus very much on the question of technical infrastructure.

So the norm that we propose is as follow, and I quote – you can read it there on the screen as well – "State and non-state actors should not pursue, support, or allow cyber operations intended to disrupt the technical infrastructure essential to elections, referenda, or plebiscites."

That's it.

LATHA REDDY: Thank you, Marietje. I think we should say that, when we look into the disruption, we basically look only at the infrastructure of elections. We're not looking into misinformation or content issues because we look at essentially how the infrastructure or the stability of the Internet gets affected.

On the third norm, I'll request Bill Woodcock to present this. This is the norm for state and non-state actors to avoid tampering with products prior to their release.

Go ahead, Bill.

BILL WOODCOCK: This is, I think, inspired largely by the NSA's attacks against Cisco and similar incidents in which governments have attempted to corrupt the supply chain and introduce compromises into products in the manufacturing process; also, for instance, the [missed compromises against] the elliptic curve cryptography, which were recommend to many manufacturers to introduce into their products. This is another intentional compromise by a government of the security of the basic hardware building blocks or software building blocks of the Internet, and these compromises, because of the manufacturing quantities, wind up affecting everybody or vast portions of the Internet. They're not selectively targeted. They are not proportionate.

So the norm here is really intended to protect customers from the corruption of the devices and software that they're buying by governments. Non-state actors as well, but that's not really what it's aimed at.

So, as you can read, state and non-state actors should tamper with products and services in development and production nor allow them to be tampered with if doing so may substantially impair the stability of cyberspace. Weasel words in there at the end because, as has been pointed out, there are many politicians involved in this process and not so many engineers.

Back to you.

LATHA REDDY: I now move onto the next norm, which is the norm against commandeering of ICT devices into botnets, by Olaf Kolkman to be presented.

OLAF KOLKMAN Yes, Olaf Kolkman. I work for the Internet Society. That's my day job. So the previous norm was about the manufacturing process. This norm is about devices that are out in the open. The norm is really about devices that could be weaponized en masse and used in attacks, inspired by, for instance, the attack that took out Dyn a couple of years ago and the fact that we have an enormous amount of unsecured devices, IoT devices, in the field, that, if they would be collectively used and weaponized, could cause huge instability.

Not only that, but if that is happening, the users or the owners of those devices might be compromised as well. They might be seen as belligerent. They might be seen as consciously taking part in attacks. And that might result in them being seen as involved in military operations.

So in order to capture that in a norm, we said state and non-state actors should not commandeer other ICT resources for use as botnets and similar purposes.

The commandeering speaks to the targeted and [proportioned], so to speak, to the en masses nature of use of this. Of course, botnets and other similar purposes, because not every attack might be instigated as a botnet – there might be other types of attacks as well – are captured there as well.

So with that, exactly two minutes.

LATHA REDDY: Thank you, Olaf. Next we move onto the norm for states to create a vulnerability equities process. Chris Painter will present that.

CHRIS PAINTER: So this is in reaction to attention that I think a lot of people have seen between states having access to [unpublicly]-known vulnerabilities where there's a tension between them keeping them for law enforcement or other national security purposes or disclosing them to make the infrastructure more safe generally. We recognize there are challenges on each side.

A couple of countries have started going down this route of creating a procedurally transparent framework with all the right stakeholders in play in the government – not just the national security agencies but also the economic and other agencies – to look at these vulnerabilities and make a decisions about

disclosing them, with an important part of this that the default presumption should be in favor of disclosure, as noted there.

The U.S. now has this process. The U.K. has recently followed suit. If I read the article I saw about Canada, like, last night, [correctly], I think Canada is also doing it. We think the more countries that have this – we're not suggesting a worldwide integrated one, although maybe that's something in the future – taking account of these various equities, I think the safer we'll all be and really doing a real balance. But, again, the default presumption is in favor of disclosure.

LATHA REDDY: Thank you, Chris. Could I move onto the next norm, which is to reduce and mitigate significant vulnerabilities? Jeff Moss will present that.

JEFF MOSS: Yeah, interesting. Hello. Thank you for having us here. This is the first norm that pretty much – all the norms before this talk a lot about the role of government – is really focused at manufactures and maybe Civil Society: producers of technology. The goal here is to become more transparent and acknowledge the accountability you have as a producer for critical systems to try to reduce vulnerabilities that may impact the Internet.

So I apologize. It's one of the longer norms. I could probably have squished it down a little bit more with some more time.

So I'll just read it for people who can't decode that. Developers and producers of products and services on which the stability of cyberspace depends should prioritize security and stability, take responsible steps to ensure that their products or services are free from significant vulnerabilities, take measures to timely mitigate vulnerabilities that are later discovered, and to be transparent about their process. All actors have a duty to share information on vulnerabilities in order to help prevent or mitigate malicious cyberactivity.

There's only a couple of points I'll point out. One is that it acknowledges that are bugs are a fact of life, vulnerabilities are a fact of life. We're not calling on people to produce bug-free software. We're just saying you should take process to reduce bugs, and when you find them, you should be transparent about them because a bug to one person or the maker might be very insignificant, but you may not realize that your software has been used somewhere else in the world that makes your bug very significant.

Because you don't have global knowledge of every way in which your technology is being used, you should assume that it has

impacts beyond your knowledge and therefore you should be transparent, when you do find and repair and remediate.

Finally, this norm sits in between two others, between the no tampering norm and then there'll be a hygiene norm. This is squished in between about how manufacturers should behave. Thank you.

LATHA REDDY: Thank you, Jeff. We move on to the next norm, which is the norm on basic cyber hygiene as a foundational defense. It'll be presented by Abdul-Hakeem Ajijola.

ABDUL-HAKEEM AIJIJOLA: Thank you very much, Ambassador. Ladies and gentlemen, the success of our evolving digital society can only be achieved when public confidence in its cyber platforms is enhanced.

Today, data is the foundational component of cyber power, influence, wealth and, indeed survival. As our society grows ever more dependent on the strengths and unfortunately the weaknesses of cyberspace, we risk building a future upon a capability and a capacity that we have not fully learned how to protect.

The key to providing effective protection is getting our foundational defenses right. Therefore, the GCSC norm on basic cyber hygiene as a foundational defense affirms that states should enact appropriate measures, including laws and regulations, to ensure basic cyber hygiene.

The GCSC norm on basic cyber hygiene as a foundational defense endorses the widespread adoption and verified implementation of a regime of foundational measures that represent prioritized essential tasks to perform and defend against, prevent, and rapidly mitigate avoidable dangers in cyberspace. We believe this norm will be of particular interest to ISP-related registries and registrars among many, many others.

Ladies and gentlemen, hygiene regime should incorporate reliable measures of implementation, provide for widespread sharing of technical information and good practice, and be subject to appropriate oversight.

Indeed, if we use the stream as the example, wanton pollution upstream will likely impact users that consume services downstream. Increasingly smart devices and processes demand smart laws and regulations.

In creating more accountability for this basic duty of cyber care, governments should not curtail innovation or confound with the basic properties of the Internet. Cyber hygiene and good practice

already exist in various forms, and they have been getting wider traction and international acceptance.

However, we must understand the importance of taking steps to demonstrate and help prevent and rapidly mitigate known dangers of malware. Facilitating awareness and [inherence] remains a critical hurdle to be overcome, due in large part to the challenges of user access, insight, and capabilities.

Bill Clinton once said, "If we could cure AIDS with a clean glass of water, we could not deliver that cure to half of the people to Sub-Saharan Africa," where I come from. Definitely, those people need help.

As of January 2019, Nigeria alone has 108 million citizens online. Of course, there are many, many more citizens online in India. Sadly, today we face the equivalent of Bill Clinton's admonition in much of the developing world, and thus the need for conveying and complying the GCSC norm on cyber hygiene as a foundational defense.

Furthermore, cyber hygiene applies to the challenges of the emerging automated technologies and determining those bear responsibility for the impact of those technologies. Potential digital realms, cyber [niches], and great advances in human well-being are being lost because we are not able to keep our digital resources healthy and available for a greater digital future.

It is therefore important, ladies and gentlemen, that states should enact should appropriate measures including laws and regulations to ensure basic cyber hygiene. Thank you.

LATHA REDDY: Thank you, Abdul. The last norm we'd like to present is the norm against offensive cyber operations by non-state actors, by Frederick Douzet.

FREDERICK DOUZET: Thank you. So this is a norm that says non-state actors should not engage in cyber operations, and state actors should prevent and respond to such activities if they occur.

The reason why we did this norm is because some non-state actors, mainly private companies, tend to advocate for the right to conduct offensive cyber operations across national borders, and they often claim they need to do that for self-defense because they consider that states to not have the capacity to adequately protect them against cyberattacks. These offensive operations are sometimes called active cyber defense and, in their extreme form, hack-back.

We've also witnessed that some states are unable to control or at least to closely monitor these practices, or they sometimes

choose to actively ignore them. In other states, they appear to be neither clearly prohibited nor explicitly authorized.

In addition to that, some states have decided or proposed legislation to allow offensive operations by non-state actors in their domestic legislation.

So the GCSC believes that these practices are likely to undermine the security and the stability of cyberspace, and they can result in serious disruption and damages. They can also trigger complex international legal disputes and escalate conflicts.

We've based this norm on international law and particularly two principles that were key to the elaboration of the norm, and that arrived from the principle of state sovereignty; on the one hand, the rights, which is that states have a monopoly on the legitimate use of force, and that's strictly bound by international law, and also on the duties and responsibilities of states and mainly the principle of due diligence, meaning that states should not knowingly allow their territory to be used for acts that are contrary to the rights of other states.

LATHA REDDY: Thank you, Frederick. So you've heard our eight norms being presented. Before we conclude our presentation, I'll call upon my Co-Chair, Michael Chertoff, to talk to you about a definition and

the principles which we follow in the GCSC, particularly on the question of cyber stability because, as you see from our name, we are the Global Commission on Stability in Cyberspace. So we see that as our fundamental mission, and I think Michael will give the summing up reports on this. Thank you. Michael?

MICHAEL CHERTOFF: Thank you, Latha. So our working definition at this point is something like this. Stability in cyberspace is the condition where state and non-state actors can be confident in their ability to use cyberspace safely and securely because the availability and integrity of services in cyberspace is generally assured.

Now, let me unpack that a little bit for you. We're not attempting here to say, "Do nothing bad on the Internet." We're talking about things that affect the stability of the Internet, including the perception of stability because of the recognition that, if people don't have confidence in the stability of the Internet, it's as if the Internet is unstable whether or not their lack of confidence is accurate or not.

Second, we're talking about injuries or threats to stability that are general in nature. We're not naïve. We recognize that, for example, there are legitimate reasons, sometimes, for nation states to specifically target a very narrow target range. That doesn't affect general stability.

But if you look at the norms we've gone through, they are focused on the kinds of activity that would undermine the general activities of the Internet, whether it's the protocols or the infrastructure or even the end points taken en masse. The idea is, if these things are compromised, then it shakes faith and reality of stability in the actual system.

So, our hope is that these norms will be taken up by governments and by the private sector in order to create an environment which we can be confident the Internet will be around and will be functional in the future.

LATHA REDDY: Thank you, Michael. I'll turn this over to Olivier at this point, if you'd like to moderate the Q&A, Olivier.

OLIVIER CREPIN-LEBLOND: Thank you very much, Latha. So now we're opening the queue for questions. For those people at the table, if you can put your tent card up if you have a question, but of course we've got roving mics, I think. We should have roving mics in the audience if anybody wishes to comment, ask a question, or make comments or so on. Just put your hand up and Gisella will come over to you with the microphone.

So I'll start the queue. I think I say Hadia Elminiawi being the first person to have put her tent card up. Then I'll go through the people in the table and we'll alternate with people in the audience as well. Thanks.

HADIA ELMINIAWI: My comment actually was with regard to your norm – I can't remember which number it was, but it's the one concerned with tampering with manufacturing products. When you see that a law coming is our legislation is coming out that requires companies to hand in end-to-end encrypted data, well, that actually forces companies to leave back doors in their encryptions or related to their cryptography. So that actually is not a direct state or non-state tampering with manufacturing, but the law in itself forces that kind of tampering or, let's say, the choice of manufacturers to do that to their products.

So how does your norm fit in with such situations? Thank you.

OLIVIER CREPIN-LEBLOND: Thank you, Hadia. Who's going to take this?

UNIDENTIFIED MALE: Jeff.

OLIVIER CREPIN-LEBLOND: All right. Jeff?

JEFF MOSS: Two general observations on that. One, we have spent an amount of time talking about, if governments propound certain requirements like that, like a cryptography backdoor, that doesn't make the company any money. So the engineering staffs in these companies, like in Apple, generally try to engineer themselves out of that problem. They don't want to have a lot of staff fending of legal requirements.

So, two things. One, I would not surprised if [these] manufacturers specifically design their products to get away from these problems because it's no-win scenario for them.

The other one is a general recognition of people who collect data that basically don't collect the data if you can't protect the data. It might also go back to some norms around transparency. If you are forced to put these back doors in, as, say, the law in Australia, everybody knows that now. So the consumers are essentially going to route around the Australian products.

So I think there are several market forces that are going to minimize the – I don't think governments are going to get of this what they thought they were going to get out of it. They're going

to make their companies less competitive. The markets will go somewhere else. They're going to be a lot of legal challenges.

So I think if you take our norms as a whole, you can see that we acknowledge that the international community is not rallying around these concepts.

BILL WOODCOCK: Yeah. I think that sums it pretty well. I think the problem that you're describing is one that we understand, and the approach of governments that do require this of manufacturers, as Jeff said, is wrong-headed and contradicts the spirit of the no-tampering and the—

[JEFF MOSS]: Vulnerability.

BILL WOODCOCK: The vulnerability norms. The norms don't try to be explicit to the last detail. They don't try to describe every possible violation. They're broad conceptual things. So, yes, it feels like that is an attack on both the supply chain and the vulnerabilities in products.

OLIVIER CREPIN-LEBLOND: Thank you, Bill. That was Bill Woodcock for the transcript. You do have to say your names because we've got the interpretation as well.

Let's go over to the floor and ask more questions.

RICARDO HOLMQUIST: Hello. If you don't mind, I will speak in Spanish.

The translators have to work.

Good afternoon. These various norms look very good, but there are different factors involved here. We are talking about very large companies in case of the norm we see on the screen. Then we have in many cases governments. But in some cases such as applications, we're talking about very small businesses and companies.

So how does your commission expect this to be implemented at the level of governments, at the level of companies? The Budapest Convention on Cyber Security – how is it related? So how are you considered in the next steps? The norms are very good. So what are the next steps? How would this be somehow enforced. Thank you.

OLIVIER CREPIN-LEBLOND: Christopher Painter, please.

CHRISTOPHER PAINTER: I'll start. Others may want to talk. That's exactly what our commission is now – it's one of the issues we're now dealing with. So we have this set of norms, which is, I should note, meant to supplement other norms that are out there, including those that came out of the U.N.

One of the things our commission is talking about is accountability and potentially enforcement. Those are difficult issues. I think we all recognize that norms alone aren't enough because, if no one actually obeys those norms and there's no accountability, they're just pieces of paper.

So they're hard issues of how we get around this, but this is exactly what we're looking at now as part of a larger framework. [inaudible].

OLIVIER CREPIN-LEBLOND: Frederick?

FREDERICK DOUZET: If I could just mention, if you look at the Paris call, there are already two of our norms that are acknowledged. I don't remember – 60 something states have supported the Paris call,

and a number of also private companies. So I think we probably have leverage.

OLIVIER CREPIN-LEBLOND: Mariatje?

MARIATJE SCHAAKE: Thank you. I just also think that one of the reasons why we're here and we're so grateful to be here is that we hope that you, as Civil Society, different stakeholders, will actually embrace the norms that you believe are useful and will convince governments, private sector companies, and others will start moving towards acceptance and, after acceptance, accountability, if there's a violation.

So this is certainly never intended as a sort of monopoly process for the people at the table here. We've done a lot of thinking. We come from very different parts of the world from very different expertises, and we've tried to crunch our heads around what we think would be truly helpful no towards the stability of cyberspace and also the trust for people in cyberspace worldwide.

OLIVIER CREPIN-LEBLOND: Olaf?

OLAF KOLKMAN: If I may say that in a different way, we cannot do this alone. We need companies. We need states. But we also need all the other actors. So, yeah, this is a call.

OLIVIER CREPIN-LEBLOND: Abdul-Hakeem?

ABDUL-HAKEEM AJIJOLA: If I may use a different tact, for the Christians here, there is something in the Ten Commandments that says, "Thou shall not commit adultery," and that you only have one wife. Now, as a Muslim, I can tell you that thou shall not commit adultery either, but I'm allowed for wives. So answering the question of whether it's a large company, a small company, the norm still applies. Thank you.

OLIVIER CREPIN-LEBLOND: Thank you. A wonderful thing. Okay. Let's alternate between the table and the floor. So the next person at the table is John Laprise.

JOHN LAPRISE: Thank you. So I'd like to ask the panel why there's no a call to protect the electrical infrastructure. I'll ask that with the

knowledge that – I'll put on my academic hat – 40 years ago, back in the U.S. during the Cold War, the National Security Telecommunications Advisory Committee said that, essentially, the telecommunications system and the electrical system we co-dependent because they relied on each other for controls, and, if one goes down, there's no telling whether we can keep the other one up.

Here it is not so different, even in this day and age. So the question is, if the Internet is co-dependent with the electrical system, why is there not a call to protect the electrical system within the norms?

OLIVIER CREPIN-LEBLOND: Thanks, John. Chris Painter and then Bill Woodcock.

CHRIS PAINTER: So I'd say a couple things. Chris Painter for the record and also, not for the record, still Chris Painter. I'd say with respect to that that I said there our norms weren't the exclusive ones out there. There were also ones that came out of the group of governmental experts in the U.N., including one against attacking critical infrastructure of which the electrical grid is part.

So I think we are, again, discussing this, but I think we embrace those norms, too. Whether you need to single out the electrical

grid as a supporting things for the Internet, I think we then start to choose among our children which critical infrastructure is more important than the other. No one had really addressed the core of the Internet as – some people might say that's critical infrastructure. Some people might say it's not. So we thought we were adding something to the debate there.

We certainly also, I think, think the critical infrastructure at large, including the electrical grid [inaudible] the financial system and others should be protected. So it wasn't meant that we don't care about that. It's just it seems to be covered by some things that are already out there.

OLIVIER CREPIN-LEBLOND: Bill Woodcock?

BILL WOODCOCK: So, in 2017, we conducted an exhaustive survey of experts of what infrastructure is needed to be protected, and the electrical grid was very high on that list. We brought it back, and we chose among our children and arbitrarily chose for of them: naming and numbering, the routing, the cryptography, and cables. So electrical was in there and was not one of the chosen children, along with quite a lot of other things that the technical community continues to ask why they're not in there.

OLIVIER CREPIN-LEBLOND: Michael Chertoff?

MICHAEL CHERTOFF: I think the only thing I would say is that we try to be very focused on things that were unique to the issue of how the Internet operates. First off, it's a good thing to protect infrastructure. That's covered by a lot of existing rules. I was Secretary of DHS, so I know that very well.

But the idea was to be very focused and add something that was not being covered by other things.

OLIVIER CREPIN-LEBLOND: Thank you. I'm going to ask for answers to be short because we've got about seven – eight – people in the queue still. Olaf Kolkman?

OLAF KOLKMAN: I think it's important that it's not only the physical infrastructure – wires and change points and electricity – but it's also the logic infrastructure. It's the routing tables. It's the standards.

So in that sense, this is fairly new, to think also about what are the intangible structures that we don't want to see messed with.

OLIVIER CREPIN-LEBLOND: Thank you, Olaf. So the gentleman to the front in the audience, I think the mic is coming over to you.

ABDULKARIM OLOYEDE: Thank you very much. My name is Abdulkarim. I want to commend for these norms. But there is one thing which I think is important that is missing in your norms which I want to find out why it's missing. It's the issue of privacy. Is there any reason why you've left that out?

[LATHA REDDY]: I just wanted to say that, if you look at our mission, it's to keep cyberspace. Privacy and data privacy – the question of data mining, how data is used – is a very big issue. But it doesn't actually affect whether or not the Internet will function.

So, from that point of view, I think it's not that we're not aware of the problem. It's obviously a very serious problem which can affect how we feel about cyberspace and how we feel about using the Internet and so on.

But I believe that this would not actually make the cyberspace unstable. If your privacy is invaded, it's a different question but a very important question. Thank you.

OLIVIER CREPIN-LEBLOND: Wolfgang?

WOLFGANG KLEINWAECHTER: We had a discussion today about the how role of human rights has an effect on stability of cyberspace. Certainly, there's an interrelationships. That means massive violation of human rights have negative effects on the stability of cyberspace. We have not yet cleared how this point should be translated in concrete language, but there is an interrelationship between respect of human rights and the stability of cyberspace.

OLIVIER CREPIN-LEBLOND: Suen Ojedeji at the table.

SEUN OJEDEJI: Thank you very much. I'm speaking as typical as an end user here because as the audience here you are speaking to. I'm just curious. Why is, regarding the actions of the [inaudible] against Internet infrastructures that consist of what we call Internet shutdowns or service denial, not reflected on the list? If, one way or the other, it's covered in one of the norms that you stated, which one of them is it?

The second point I wanted to make is I think it's very good that there is really a way to actually see the effect of these norms. So if you may, you may consider having a way we can track what the effects are exactly somewhere. Thank you.

OLIVIER CREPIN-LEBLOND: Any response required? Go ahead, Jeff.

JEFF OSS: I'll just start and pass the bill. So I think we all agree that, in your – if we understand correctly, you're talking about a government or a country taking itself offline, which we would consider an attack against the routing infrastructure. So there is discussion about how we operationalize some of our norms. Some of that may be a hat tip toward the certificate transparency community or the EFF's Internet Observatory. Or maybe we are talking about possibly a norms observatory. Which countries or companies have signed up to these principles? Which companies seem to always be violating them? Which countries seem to always be violating them? Because I think the first step towards socialization around these norms is you have to identify who the good players and who are the bad players.

So we're hoping through a partnership, not us but through finding appropriate partners, we may be able to get some

operationalized observatory around these concepts. That's a new idea for us.

BILL WOODCOCK: Yeah. I think there are two axes here. One is whether a country or an organization has expressed adoption of a norm. The other is compliance or adherence. So I think we can track both of these things. It's easy to track who has said that this norm represents their understanding of their behavior. We have some 60-odd countries already there – essentially every European country, half a dozen in the Americas, half a dozen in Africa, half a dozen in the Asia-Pacific region.

Then we have to look at whether countries are doing things that violate these norms because someone could say that they support the norm, but then their intelligence agency or their military could go out and violate it. So we need to track these two things separately.

OLIVIER CREPIN-LEBLOND: Thank you, Bill. I think we're going to have to go through the questions because we still got four people and ten minutes left. So we'll go a little faster.

Elliot Noss, you're next.

ELLIOT NOSS: Hi. I really want to commend all of you on this work. I've been publicly hoping for what I would call a multi-stakeholder process on cybersecurity, and this feels like the genesis of it. In that regard, I'd really like to encourage you all to do a couple things.

One, please make sure that you stay separate from this process. By that, I mean ICANN has its very particular remit. You have yours. And I think they're both equally important and separate. Multi-stakeholderism will thrive when there is a vertical focus to it.

Two, leverage this community and this work. I think you could do that in a couple ways very specifically. The first would be to come to these meetings on a regular basis. I think that one of the benefits that you could get from that is that there's significant presence of law enforcement here from around the world. That was one group, at least according to your little diagram on the front page, that is not currently actively part of your multi-stakeholder process.

I think, for you to generate real effect and to have your remit increase over time, you will have to have law enforcement as a necessarily part. Law enforcement may be to you guys, in terms of cybersecurity, what the GAC has been for the ICANN

community, where it's first starting outside at meeting in private rooms and slowly, slowly, slowly becoming more integrated.

This is going to be a long process, and I'd really encourage you to leverage as much of this as you can. Thank you. Now I have to go to the Registrar GAC meeting, ironically.

[LATHA REDDY]: I just wanted to say that I thank you very much for that. And you'll be happy to know that six of our commissioners have at some stage had extensive interaction with ICANN. So we're very well aware of what ICANN does, and I think we've got the necessary traction for the leverage.

But your point is well-taken, that we shouldn't let ourselves be subsumed into the ICANN process. Thank you.

Anyone want to – Olaf?

OLAF KOLKMAN: Yeah. One of our commissioners actually is a leader in Interpol, so we have that captured within the commission.

On the multi-stakeholders, it's very clear to us that there are multiple approaches to multi-stakeholderism. It's also very clear to us that this is a community that has a very specific mandate,

but we believe that the public core norm very much attaches to that mandate.

Thirdly, what we've been trying to do with the commission is to go to several places where the constituencies and our backgrounds are. That doesn't necessarily include law enforcement, but it does include, for instance, the more military side of cyber stability and the more political side of cyber stability.

So we've been trying to reach out and position the norms and get feedback. Also, in my own community – the Internet Society community – we've been trying to do that. And that's [what we hear.]

The problem is that we have a mandate that is lasting for yet another year. So getting deeply involved in the ICANN process might be a little bit of a challenge there.

OLIVIER CREPIN-LEBLOND: Okay. We do have a hard stop at quarter past, so what we're going to do is take all the remaining questions. Then you can address them and then we'll have to stop and perhaps follow up as a follow-up to this meeting.

I've got Jonathan Zuck, I've got Holly Raiche, and still the gentleman also. So we'll alternate again: table, audience, table. Go ahead, Jonathan.

JONATHAN ZUCK: When Ms. Reddy was talking about interacting, I thought you were going to say law enforcement, and that was about to get really interested – what that might have meant. But I'm glad that you're talking about some things like naming and shaming potentially because my concern about norms obviously is one that you share which is, what will become of them? It becomes a little bit like arms races, where everyone is saying, "You first," etc., and it becomes a difficult thing to happen simultaneously.

I try to think of examples in history, like the Sullivan Principles, or something like that, that might be an example where there was enough public pressure to bring people along incrementally.

But one idea [you] might plan is to try and get the norms taken up by an organization that already has an infrastructure of compliance and enforcement. So I'm hesitant to say it, but an organization like WTO, for example, is one where there's already teeth in that membership. A lot of these things could be construed almost as constraints of trade. So are there organizations like that that already have infrastructure for

monitoring enforcement, etc., an organization that people feel invested in? That might be a good outlet for the norms.

OLIVIER CREPIN-LEBLOND: Thank you, Jonathan. The gentleman next to Nigel Hickson? Please introduce yourself.

[NANO DORWICH]: Yes, I will. Hi, my name is [Nano Dorwich]. I come from Serbia, and I would like to direct my question to Frederick Douzet. To my knowledge, ICANN participated in at least one, and Microsoft in several, operations to identify and take down a large number of domains that were used for botnet for cyber virus extortion rings.

The question is, would their inclusion in such an operation be against the norm you presented?

OLIVIER CREPIN-LEBLOND: Thank you for this question. We'll give Frederick a few minutes to think about and answer this one. We'll then go to Holly Raiche for the last question.

HOLLY RAICHE: Holly Raiche from Australia. I think I would like to ask all of you what did you do about the Assistance and Access Act of 2019? Did

you make any submissions? Have you made any statements? I'd certainly welcome it if you haven't.

OLIVIER CREPIN-LEBLOND: Thank you, Holly. In Australia.

[HOLLY RAICHE]: [Terrible].

OLIVIER CREPIN-LEBLOND: Okay. Let's go to Frederick Douzet.

FREDERICK DOUZET: To answer the first question, I don't think we want to go as far as naming and shaming because that would involve doing attribution, and that's very political.

I think the goal of monitoring norms violations is more in order to understand trends, whether we're making any progress with cyber stability.

It's also providing legal analysis about past cases in order to build up cases that help understand how international law applies to cyberspace and monitor which norms are being respected or violated. So it's more in sense, I think, that we want to do it.

As far as taking down botnets and leading operations, again, the idea is that states have the monopoly and the legitimate use of force, so it all depend on whether you're doing that because the state asked you to do it or whether you're doing that on your own.

We think that, if the state authorizes you to do it because there's a need to do it, then you're considered a state agent, and therefore, under international law, the state in considered accountable.

OLIVIER CREPIN-LEBLOND: Michael Chertoff?

MICHAEL CHERTOFF: As it relates to the third question, I take it you're talking about Australian act that requires backdoors and encryption. We have not gotten to the point yet where we would make submissions because we've not fully voted on all the norms. But I think you could make a pretty good argument that the norm about not inserting vulnerabilities embraces this issue.

I suspect this is going to linger for a while and we'll have an opportunity to weigh in. One of the things we do hope to do once we finalize our final report is to get engaged in advocacy and deal with situations where legislations are doing things that we view as incompatible with the norms.

OLIVIER CREPIN-LEBLOND: Thank you, Michael. Finally, Chris Painter.

CHRIS PAINTER: Thank you. Just to add to Frederick, as I understand what Microsoft has done, they usually do it pursuant to court order. So they do these takedowns and they work with other governments. So I don't think it would be prohibited by our norm.

On the naming and shaming issue, I think part of it is the observatory calling out violations, but we also have to think about – the commission can't do this itself – how there's better enforcements of the norms we have or the expectations we have because I think most of us see the trend getting worse rather than getting better. Even with the proliferation of some really good norms out there, it doesn't seem to be on the upward trend. So we have to figure out how to change that.

OLIVIER CREPIN-LEBLOND: Thank you for this, Chris. Any other comments? Marietje?

MARITJE SHAAKE: I just wanted to briefly build on what you said about seeking existing institutions, where enforcement and buy-in by states already exists. This is definitely the line of thinking that we're on,

but we haven't fully worked out yet the question of observing norm adherence and the question of attribution and the question of accountability. But I think your point is very well taken, and it's definitely the line on which we are.

So you can also see from my answer that we don't think we're finished. This is still very much being deepened and worked out. We work very intensively to consult with people for better output and to develop further the norms and the implementation that you've seen today.

OLIVIER CREPIN-LEBLOND: Thank you for this. I'm told the next guest coming in has not left their room yet, so we actually have a couple more minutes, which is great for us.

UNIDENTIFIED SPEAKER: [inaudible].

OLIVIER CREPIN-LEBLOND: You've got to go somewhere else. Okay. So some people. Okay. So Wolfgang is not going to be able to speak because he just stood up.

So let's go over and have the question from the gentleman with the beard in the back, please.

[DIEGO CANABARRO]: Thank you, Olivier. My name is Diego and I come from Brazil. I work for the Brazilian Internet Steering Committee. I just wanted to get information. Olive, actually, is leaving, but he mentioned something related to the logical layer of cyberspace. I wanted to understand a bit more about your conception of the public core, mostly because there is a huge amount of literature discussing what is public, what is private, what is [common] in Internet governance.

Apparently, most of the things that you point out as being part of the public core of cyberspace are actually in the hands of private actors: submarine cables, routing infrastructure and other sorts of infrastructure that actually lies 80% in the hands of the private sector. What would be the implications of publicizing those things by applying your concept of the public core to those private assets? Thank you.

OLIVIER CREPIN-LEBLOND: Latha Reddy?

LATHA REDDY: I think, if you look at the explanations that we put forward for the public call, we said that the technology that underpins the global Internet is imperfect. We consider the public core itself to be a

critical infrastructure. Technology can break, and the existence of flaws, vulnerabilities, malicious actors, and the development of offensive capabilities can create conditions of instability that put the benefits of cyberspace in jeopardy.

I think that we have tried to outline what are the technical elements that we feel would essentially effect the public core, would prevent the Internet from functioning. I don't think there's a value judgement that one is more important than the other. I think we essentially are looking at anything that prevents the Internet from functioning as it should function should not be attacked. And we clearly say it's both for states and for non-state actors. Our norm says that.

OLIVIER CREPIN-LEBLOND: Thank you for this, Latha. I have noticed you, Anriette So Anriette Esterhuysen, also part of the commission. So please go ahead, Anriette.

ANRIETTE ESTERHUYSEN: Thanks, Olivier. Just to answer Diego's question, because I think it's quite a fundamental question, I think the point about the public core norm is that it doesn't matter whether that bit of the Internet that constitutes the public core is managed by a private entity or not.

What matters is that it is managed in the public interest, as you would say in ICANN, or for the overall stability and resilience of the Internet. In fact, that's precisely why we address both state and non-state actors. So it's not necessarily to publicize it further. It's actually public already, even if not owned.

OLIVIER CREPIN-LEBLOND: Chris Painter?

CHRIS PAINTER: Just one other thing. We took a lot of time drafting this Anriette, than others, drafting these norms, because we understand that what we're talking about here is substantial disruptions of the Internet, not little disruptions, regional disruptions.

So to the extent that actors, governments, and others are saying, "Look, we need to do some things on the Internet," for law enforcement purposes, for instance, we're not prohibiting that. We're being clear about understanding what they need to do for their equities.

But if you do something that has a substantial disruption that hurts everyone in the community or a large section of that group, that's what we're trying to prohibit.

OLIVIER CREPIN-LEBLOND: Thank you very much, Chris. If there are any further questions on this topic, I would suggest that people send them over to staff@at-large.ICANN.org. We'll transmit them over to you and get answers in writing.

So thanks so much for coming to see us. It's a real pleasure.

LATHA REDDY: Thank you. If I may, on behalf of the Global Commission, thank you very much for your time, attention, and patience. It's been a pleasure to have this public consultation meeting with the ICANN At-Large Advisory Committee. Thank you, Olivier, for your very able chairing.

OLIVIER CREPIN-LEBLOND: Thank you. Next we have Keith Drazek, who's coming to the room. I'm going to hand the floor over to Cheryl Langdon-Orr, who's going to take this part. So please do not leave. It's ongoing.

UNIDENTIFIED FEMALE: Ladies and gentlemen, we're about to start the next session now with the Chair of the GNSO. Thank you. Please do, ALAC and regional members and liaisons, come to the table. Thank you.

CHERYL LANGDON-ORR: Ladies and gentlemen, if you would be so kind as to take your seats if you are ALAC/At-Large regional leaders. If there are seats to spare, please do come from behind Keith and I because we're paranoid individuals and we would prefer to see you. So feel free to move to the front. Take a seat at the table if you so desire.

With that, I could whisper very quietly see whether that works. Thank you.

For those of you who don't know me, my name is Cheryl Langdon-Orr. It is my privilege, without my tent card – so I don't actually know who I am – to be the ALAC's liaison to the GNSO Council. And I think it's Keith's privilege now to be the incoming, relatively new – been there for all the good bits of this year – Chair of the GNSO Council.

Why are we meeting? Well, other than that you can now recognize him and make sure he doesn't enjoy a coffee break ever again, we also have some very important things that are happening with what we're doing as an At-Large community in response to our own review of the regions in and At-Large.

Part of what we've undertaken to do is become more engaged in policy, for example, more obviously and directionally engaged in policy. Of course, at the same time, you and your lot have gone smacking off and designed a whole new 3.0. So we'd like to hear a little about how the GNSO works, because, just like a lot of your

constituencies and stakeholder groups think that At-Large is all of us or the ALAC is all of us – a little bit of structure and functions – I know that you're not just the GNSO. You're a slightly different beast.

Then take us into what's likely to happen, knowing it's still a draft, with PDP 3.0 because what we're doing is priming people to come and join more policy development, and what some of us fear is that might actually be the same option as it is now. So, Keith, the floor is yours.

KEITH DRAZEK: Thank you very much, Cheryl. Thanks for the invitation to be here with you all today. So, yes, my name is Keith Drazek. I am the new and current Chair of the GNSO, and GNSO Council as the Policy Development Process Manager for gTLD Policy Development. The GNSO Council is not me by myself.

So, yeah, I'm more than happy to talk about the structure of the GNSO briefly, talk a little bit about the evolution of the Council's engagement in the PDP process.

But let me just first say that we are very, very pleased to have members of ALAC participating in the GNSO processes. In particular, obviously the most recent examples would be in the Subsequent Procedures Work Track 5. In addition to the fact that

you are a Co-Chair of that overall PDP – so thank you for that effort and sacrifice – but also the EPDP to replace the temporary specification. And a shout out to Alan and Hadia for the incredible sacrifice. The amount of work and intensity that was required there was really Herculean. And the delivery of a final report within the timeframes required – demanded, really – by the temporary specification was really something to behold.

I know that there are still some frustrations with the work that didn't get done in Phase 1, but, as the GNSO Policy Process Manager, we are committed to ensuring that Phase 2 kicks off, that it's properly scoped, properly resourced, and that there's still a sense of real urgency to move forward on the standardized system for access and disclosure for non-public registration data, also referred to as a UAM or Uniform Access Model.

So, from a Council perspective, we are fully committed to ensuring that the charter, we believe, is still fit for purpose, but we are prepared to support the EPDP Working Group in its work to develop a work plan and to establish the expectations for that group moving forward. The GNSO Council may continue to provide some additional guidance to the EPDP Working Group over the coming weeks, but the ball is still very much in the court of the EPDP itself.

We do have to find a new chair. I think, as most people know, Kurt Pritz indicated that, after the work on Phase 1, he was stepping back and not prepared or able to move forward on Phase 2. So the GNSO Council has actually opened a call for expressions of interest for a new chair for the Phase 2 work. The timeline for that is March 22nd for a deadline. Hopefully we'll receive enough qualified interest that we can then move forward with a selection process and approve that by the GNSO Council's meeting in April, which is April 18th. So we can talk more about that.

Let me just take one step back. The structure of the GNSO Council and the GNSO generally, for those that are not familiar, is a bicameral structure. There are effectively two houses within the GNSO Council and the GNSO. There is the Contracted Party house, which consists of the registries and the registrars in two separate stakeholder groups.

Then, in the Non-Contracted Party house, we have a commercial stakeholder group and a non-commercial stakeholder group that includes essentially the range of all of the other interests in the GNSO; so from a business constituency, intellectual property interests, non-commercial users constituency, the ISPCP, the not-for-profit interests. So there's range of different views in the non-contracted party group.

So at a Council level, there's one chair that is selected from among the councilors on the group, and then there are two vice-chairs, one from each of the houses, Contracted Parties and Non-Contracted Parties. That's essentially the leadership team of the GNSO Council. Then we've got the councilors from each one of those groups.

There's a good graphic on the ICANN website at GNSO.ICANN.org that actually is a visual representation that, if anybody wants to follow up.

So I guess in brief we've some ongoing and excellent interaction with ALAC and GAC and other parts of the community in some ongoing PDP work. So we talked about Subsequent Procedures, Work Track 5. We talked about the EPDP. As I look forward – now we'll talk about the PDP 3.0 – I think there is an expectation that there will continue to be that opportunity.

One of the things that the GNSO experienced over, I would say, probably the last six or seven years, or maybe even going back longer – and I think it came to a head during the last round of new gTLD policy development that culminated in the 2012 guidebook and the work that went from there – was that we had the GNSO developing policy in a bubble and then, afterwards, having the GAC come in with advice to the Board as one example.

I think there was a recognition at that time that time that we would be more effective in our policy work had we had input and viewpoints shared earlier as part of the process.

So, going back several years now, the GNSO – I think this goes back to when Jonathan Robinson was the GNSO Chair, so that's probably three or four chairs ago now – [had] an active outreach to at least the GAC. I think now we've recognized that the more we can engage the interests and the people from the advisory committees in our policy making processes early and often, the better off we're all going to be, where we don't end up with surprises at the end, where there's advice that conflicts with policy recommendations. I think that what we're seeing today is evidence that that's actually helpful and that it's welcome and that it's delivering.

So I think, certainly during my time as Chair, I'm committed to ensuring that we have an inclusive process in PDP work and that we regularly consult with and engage with and invite anybody who wants to participate to engage in those groups.

Specifically on the PDP 3.0 question, last year, the Council, under Heather Forrest's time as Chair, there was a recognition that we had PDPs that were going on for years and years and years and in some cases years more. We had PDPs that were going on for four years and we had some that –for example, the RDS PDP Working

Group was recently shut down after having done work for three years or so. Of course, that was in part because of GDPR and because of the temporary specification, a recognition that the world had changed from when that group was first chartered.

So I think there's a recognition at the Council, last year, that we needed to do a better job as the process managers for PDPs to make sure that they're scoped appropriately, that the groups are chartered in a way that is effective and efficient – those were the two words that we rallied around; of being more effective and more efficient – in our management of these PDPs.

It included a recognition that our Council liaisons to the PDP working groups needed to be more engaged, needed to be more active, needed to be available to the working group members in the event there was a problem or a perceived challenge to the process or where a working group chair might have been operating out of the bounds of the normal procedures.

So we went through last year a process that resulted in approximately 16 recommendations for improving out ability at Council to be better managers of the process, to make sure that we don't end up with PDPs that last four years and that we end up with PDPs that are working well and that, if there's a problem or a challenge to delivery on time or the dynamics in the group itself or the leadership, we have early warning that that's the case

and that we are prepared and able to take steps early to keep these things on track.

We also recognize that there is only so much bandwidth from a volunteer perspective, from a staff resource perspective. If you're having face-to-face meetings out of band, the cost of that under constrained budgets with ICANN, we need to do a better job of prioritizing. That was one of the key words – prioritizing the work. And if something new comes in, like the EPDP, because the temporary specification, there may be a recognition at some point – there needs to be – that something else may have to be paused because there's only so much that can fit in the pipeline of the community policy development work in the GNSO and especially true if we have other parts of the community participating. We can't just look at this through a single lens of the GNSO resources and what we can handle from our perspective. It's more of a community consideration.

So I'm happy to share the recommendations that came out of last year. What we're doing this year is working through a process of implementing those. That won't be, okay, all of a sudden, all PDPs are going to work with this or we're going to do something like this. We're going to evaluate as we go through and a we initiate new policy development processes or consider ongoing PDPs.

Are there ways that we can fine tune these? Do we need to adjust the charters of some of these groups. Are there things that we can be doing better as the GNSO Council managers to ensure effective and timely delivery of the end result, which is a consensus policy recommendation to the Board.

So last thought. Happy to take questions. I'll give you an example. There's some discussion right now about what happens with the RPM PDP Working Group. This is the group that's focused on rights protection measures for all gTLDs. There's a Phase 2 work that's going to focus just on the UDRP, the Uniform Dispute Resolution Process.

There's discussion about whether the GNSO Council needs to recharter that group at the end of Phase 1 to kick off a more effective and efficient Phase 2. So that's an example of how we might be considering to implement and test some of these new PDP 3.0 stuff.

So I'll stop there. Thanks, Cheryl.

CHERYL LANGDON-ORR: Thank you, Keith. Apologies to the translation team. I promise to slow down to a speed that will allow you to just take a breath because were running when Keith was getting everything in.

KEITH DRAZEK: Sorry.

CHERYL LANGDON-ORR: It's only in three languages. Don't worry about. But, no, thank you, Keith. I'd like to get Keith out the door to his next meeting so we don't have this knock-on effect of one thing running late. So I see Jonathan in the queue. Short questions, please. Short answers even more so.

Jonathan, go ahead.

JONATHAN ZUCK: I guess on the topic of short PDPs, a couple of our successful stories we've had as a CCWG on the accountability framework and the EPDP were both externalities that created deadlines. Is part of your prioritization potentially to timebox a PDP and then redefine the scope to fit the timebox potentially in order to at least create incremental policy proposals?

KEITH DRAZEK: Short answer, yes. It's one of the things we're discussing. It's certainly a consideration. So there are challenges of establishing an arbitrary timeline in some instances, but in other instances, it actually, to your point, could be very effective. That's absolutely one of the components under consideration for our PDP 3.0.

I apologize to the interpreters.

CHERYL LANGDON-ORR: You did perfectly well there. Holly?

HOLLY RAICHE: Going back a little while to the [TSO] review, which is back there, one of the recommendations that seems to have been buried was very early collaboration between GNSO and ALAC – for example, webinars – so that, basically from day one – and ICANN's had an opportunity to listen to what this particular PDP is all about and make up their mind if they're participating, who participates. That kind of thing would be really useful. And please do at two time zones.

KEITH DRAZEK: Thanks very much. Holly. Point well taken. I think we heard something similar in my last meeting with the GAC, specifically to the EPDP charter, that there was a certain understanding or expectations or interpretations that turned out not to be maybe what was expected or understood, and there was no opportunity at that time for early input and understanding and engagement. So I fully take on your suggestion that that's something we should absolutely consider. Two time zones.

CHERYL LANGDON-ORR: Well, just make sure they're the right time zones. That helps. West and east coast U.S. is not going to be quite what we're after. I'm now going to ask each and every one of you to thank Keith in the usual way because I'm getting him out the door with a few minutes to spare. We've had a little time with you, but I think it's valuable time with you. If I may channel the group around the table, we'd like the opportunity at some future point in change to have an interchange with perhaps not just you but your leadership team and some of the leads in the GNSO Council so we can care and share a little more and build some understanding.

So, ladies and gentlemen, we have another session starting in three minutes. Keith is leaving now. Thank you very much, Keith.

KEITH DRAZEK: Thank you. Thank you, all. Thanks very much. I look forward to doing it again, expanding it, and having a little bit more time for Q&A. Thank you. Thanks, all.

[END OF TRANSCRIPTION]