
MARRAKECH – GAC: Joint Meeting with the Global Commission on the Stability of Cyberspace (GCSC)
Thursday, June 27, 2019 – 12:00 to 12:30 WET
ICANN65 | Marrakech, Morocco

WOLFGANG KLEINWACHTER: (Initial audio missing as Zoom audio was not active for scribe).
... cyberspace natural we reached the out to ICANN because
ICANN's mission and ICANN's priority is the (inaudible) and
stability and resilience of cyberspace –

ELECTRONIC VOICE: The recording has stopped.

ELECTRONIC VOICE: This meeting is being recorded.

WOLFGANG KLEINWAECHTER: -- very good conversations with members from the security and
stability advisory committee with members from the GNSO in
particular with from the NCUC and the ISP constituency and we
had discussion was the at large advisory committee but the role
of users and we are happy that we have now a chance just to
inform the governments of the work of the global commission
and normally in the GAC you have representatives from ministry

Note: The following is the output resulting from transcribing an audio file into a word/text document. Although the transcription is largely accurate, in some cases may be incomplete or inaccurate due to inaudible passages and grammatical corrections. It is posted as an aid to the original audio file, but should not be treated as an authoritative record.

of economics. Development. IT, there are some from 4 ministries but I think stability in cyberspace is an issue which goes to the government as a whole, and in so far its -- we very good if you could just inform your home governments what's going on with the commission. Here on the table we have 2 commissioners. This is Anriette Esterhuysen -- she was a member of the NomCom it's up to her team from Africa and we have Alexander Klimburg who is the director of the program and will give the presentation and we have also Philip ... a member of the management Board because ... is one of our partners so I hand over to Alex, thank you.

ALEX KLIMBURG:

Thank you. From my side of the invitation to be here. I am Alex Klimburg, a director of the global commission of stability for cyberspace. Wolfgang has introduced our members of the commission that are here today. And most of them of course are well known to you and we have been engaging with members of the ICANN community over the last year as I said we've been talking about members of SSAC, ALAC ISPCP and the ICANN Board and if you're wondering how we are we can with all the acronyms I invite you to come and participate in a UNGGE -- CCS what we talk about IL, LOAC and ICBM see we feels right at home of the mission of ICANN the mix of the GCSC is engage the full range of stakeholder others to develop proposals to enhance

international security and stability and guide responsibility state and non-state behavior and cyberspace.

So we are therefore focussed on influencing the so-called international cybersecurity discussion that's largely encapsulated in the U.N. commissioners committee processes such as the group of governmental experts and the open-ended working group and we do this by importing views from other parts of what we call the cyber regime complex. So that's the technical and the business community from the rights community and, of course, the particularly from Internet governance. We want to empower the views of these communities into the international cybersecurity discussions and basically maybe their deliberations more informed.

We build on 2 mandates. We have a rather clear cut from the 2015 global conference on cyberspace meeting in the Hague. But we also derive from the 2015 U.N. TGE report where it mentioned the need to have a better outreach and consultation process. We like to think we are that outreach and consultation process. We are very multi-stakeholder group. And we have been working on norms and policy initiatives since our launch under the patronage of the Dutch foreign minister in 2017.

We are about to finish our report. Many of you have seen some of our draft content issues that we've circulated mostly regarding norms and this will be expanded upon to include a definition of cyber stability as well as concrete recommendations how it can be best achieved. Now briefly also on who we are and a very busy slide. We are at 28 commissioners and chairs from 16 countries who have a lot of experience working on different parts of the wider cyberspace policy ecosystem these include senior state. But also Carl Bildt who was former prime minister of Sweden. We include academics like Joseph Nye and Wolfgang Kleinwachter and technical experts such as Jeff Moss, Lee, and Bill Woodcock and other people you're familiar with. We've been working also with research advisory group that has over about 100 members and who we also use to process some of our work in draft form and we are advised by our partners and sponsors who take an active interest in our work. Our partners are governmental and nongovernmental.

We have 3 government and 3 nongovernment partners. And they are quite active in our deliberations and also in delivering our product to a wider audience. One of the most visible components of the work has been on norms. And norms to remind are legally nonbinding agreements on accepted behavior such as those discussed within the U.N. GGE context. I want to share with you

one norm in particular that has been particularly seen as relevant to the wider ICANN community and that is the norm to protect the public core of the Internet. You can see the draft norm up on the screen now. And you also can see the various elements that we think constitute the public core of the Internet. These include for instance packet routing authority for the cryptographic mechanisms of security and identity and the physical transmission media. The most important part of this norm is that it effectively is the principle that it implies and that is that parts of the critical infrastructure that underpin the global Internet are effectively a global public good that deserve special protection. This is more or less agreement we are working from and this is more or less the principle accepted by a number of external stakeholders in a number of endorsement we have received externally.

There is also the norm that we are discussing most with members of your community. Most particularly on the definitions of what for instance these various elements mean. And the way we usually approached it that core aspect of the public core, the packet routing and forwarding naming and number system is concrete and easy to define and it gets more squishy the further out you go. And this outer definition of the public core is also what we are trying to help define but the inner part of the core is

something that is core, of course also to ICANN mission does include of course the domain name system as well as routing protocols and similar. I would have course encourage you to pick up some of the print-outs we have here. They should be available and visit our website for additional information on this particular norm. We have, however, worked on other -- norms to protect the public core of the Internet was chosen because we thought when we looked at existing U.N. GGE norms our focus was not to replicate what was already done but to find the gaps.

One of the gaps was there wasn't enough norms that were critical of cyberspace so critical for cyberspace to function. So norm to protect the public represents the first attempt to define something critical to the public core of the Internet to function and our next was to define an example of a critical service that is run in cyberspace, and one of course can always choose the power grid but a lot has been said on that so therefore our second norm which is for and the right was a form to protect the electoral infrastructure. This is by the way of all elections irrespective of how democratic the national political system is and it does not look at content. It's regarding the infrastructure that underpins the decision-making processes. In between these 2 norms we have hope to be able to map out the stability of cyberspace. The number of other norms we won't have time to go into today but

those include for instance a norm to avoid tampering an ICT products in production.

A norm for states to create a vulnerability acquitted process, a way for disclosing vulnerability a way of commandeering devices into botnets. A norm to reduce vulnerability at production. A norm on basic cyber hygiene, a norm against offensive operations by non-state actors. All these can be looked up on our website. These are the rough title. They have one thing in common. They apply mostly not only to state actors but also to non-state actors and there is also where our work has been more unique than the work that's been picked up for instance in governmental circles is that not only are we multistakeholder, we also multistakeholder in our orientation and audience. We have been therefore endorsed by a number of different partners who have a similar orientation. The Paris call that was issued last year by President Macron picked up 5 of 8 of our GCSC norms.

We are active in the formulation of this call and it makes special reference to the public core of the Internet. This is also I like to point out a call that has since been signed by 547 like-minded states companies and civil societies organizations. So this includes also a large number of the world's governments and including 4 out of 5 of the so-called 5I government as well. We

also have had quite a lot more success with the norm of the public core within the context of the EU. Today is a very special day because today the EU cybersecurity act which is one of the biggest steps in EU legislation is going into force. And in that E cybersecurity act the public core is not only mentioned but it is made also a responsibility of the new agency that the takeover from the European network information security agency. For those of you not aware it is being upgraded and a mission is to help research and protect the public core of the open Internet. The tech accord, a group of companies that is mostly followed leadership of Microsoft in developing norms welcomed our work and made special references to a norm of our norms including a [inaudible] and the norm of state to create a VAP.

Finally, we are not only working on norms as I said before. We have been using the norm work to help influence our thinking on what cyberstability is. That is not only a definition. But it's also connected with principles as well and as final stage recommendations both to state and non-state actors. So we are currently working on this as our draft definition as a -- as a what cyberstability comprises but as I said before. All of our work actually even though we've circulated it widely is actually in draft form. Our final report is coming up in November. And in that final report we still are going to be including a number of views

including the views gathering here today. So I'd like to close with a simple reference this is not the -- this is not the beginning of the end but is a more or less the end of the beginning of our process. Next year we will be concentrated on implementation and support of our norms and recommendations.

This is the chance to help further define what for instance the public core means in the context of the EU. This is so-called secondary legislation the. The public core now is out there as a term. And as a principle. Exactly what it means is now up to all of us here to help define. And I like to turn lack to our chair and also to the commission others to answer your questions. Thank you.

MANAL ISMAIL, GAC CHAIR: Thank you very much. Thank you Wolfgang and thanks Alex for this informative presentation and for reaching out to the GAC for their views. I see a request for the floor from MALI.

MALI: (Interpreter). The representative of Mali speaking. I have a question, and a comment. My question is the following. I would like to know if the IP ... deployment will have an impact on the -- on cyberstability. That's my first question. And my comment is the following. I do not understand when you say that IPBC will make

it possible to international prove on-line traffic and will make things change or different, I am a physician by training and I would like to know how I can use devices in the Internet of things for my profession, given that IPV4 addresses our... resource and the different band width issues so what's your vice to governments in this regards? What could governments do or impose in terms of the net? What could we integrate to IPV6 so that we can resolve those problems. Thank you.

ALEX KLIMBURG:

Well, our commissioners just a quick answer to that we effectively endorse the best community practices be adhered to. That's the underlining, underlining premise of our work and we also underlying always propose governments draft regulations and advisory notes that are based upon defendant community practices. And a technical example if the community thinks BCP38 and similar technical fixes are something that should be proposed I suggestion taken up by the community we think governments should adhere. We don't normally go into the level of detail of saying IPV6 DNS or other things should be adhered to but rather the best practices should be adhered to. I would like to can ask the commission others to comment.

WOLFGANG KLEINWAECHTER: Yeah, thank you for that general comment on this because what I have observed over the years is that regardless of the lip service for the multistakeholder model we see that various communities are still working in silos. In particular the silos for the code makers on silos for the lawmakers, and this is our commission also encouraged to build better bridges between the various silos so code makers and lawmakers are working hand in and hand to find out the best solution for specific issues. We all know there are no silver bullets so you have to build solution around a certain issues and you know probably for your economy it's different phone for your law enforcement and it means to go case by case. Issue by issue and develop a button up multistakeholder consultation process in your country is the best way to find out the right solution.

ANRIETTE ESTERHUYSEN: I can add as well. I think that you know we, our norms –

MANAL ISMAIL, GAC CHAIR: So sorry to interrupt. If we can identify who is speaking for the transcript –

ANRIETTE ESTERHUYSEN: Anriette Esterhuysen, one of the commissioners. Thanks, Manal. We are actually trying to use norm as a common language

between different processes and communities, and we also are trying to fill gaps in norms address cyberstability particularly after the group of governmental expert process of 2017 did not produce new norms and we are approaching in the case of IPB6 there are lots of norms andv... recognized more broadly so there's not a specific need. We feel for us to address IPV6 deployment but we have to take it into account. We are trying to do is to find norms that create a bridge between stakeholder groups. Between binding law and nonbinding common understood standards of good behavior. Between technical policy and public policy, between developing countries and developed countries. So we using norms as a way of filling gaps. Building bridges. And creating a common understanding of what our key approaches and requirements necessary for cyberstability more broadly.

MANAL ISMAIL, GAC CHAIR: Thank you, Anriette. I think we have one more comment from the –

ABDUL-HAKEEM AJIJOLA: I think we have to understand that in terms of IPB4 the address ability space was 4.8 billion addresses. And with IPV6 we are looking at 3.40 times 10 to the power of 38. Which is about 340... spaces now that means obviously that there's significant room for future expansion. And I think also you will find that IPV6 is a

little more efficient, in fact, much more efficient and definitely security has been baked in much more significantly at its core. Sometimes because of the addressing problems you know different ISPs have to use network address translation. Not that it's bad but it does have significant challenges including speed. Now having said that I think that for you -- you to look at the GCSC norms as a toolbox. What I point you to is one thing Alex mentioned. The new EU cybersecurity law that incorporates one of these, in fact, the core -- the public core norm takes effect today. And so coming from the south south, my question is, what can you take back home from our work to incorporate into your government thinking and planning and so that is what I would encourage you to do, to really own the norms. Because we sunset, arguably at the end of the year and it's not about us. It's about how you can leverage our work to your best advantage. Thank you.

MANAL ISMAIL, GAC CHAIR: Thank you, Abdul-Hakeen. I can see several requests for the floor. Maybe take a few questions and then allow the panel to answer. So I have U.K. I have Argentina. I have CTU. Indonesia. Okay just let me -- U.K. Argentina CTU. Indonesia. Congo. Okay, U.K., please go ahead.

UNITED KINGDOM: Thank you. Paul Blaker for the U.K. government, and thank you to the panel for coming here today and for the presentation. I think in the U.K. we found this consent of a public core quite difficult to understand we did sign the Paris core and we support the good intention behind this norm. But we did express some reservations because we are not sure how helpful or meaningful the concept of a public core really is. What -- it's not quite clear what do we mean by a core to the Internet. The Internet is a network of Internet works so do we just mean the DNS, or protocols. You talked about an inner and outer core. Which might include physical infrastructure. So it's not clear what we mean there. We are not sure what it means by public either but much of what we understand as the Internet is privately owned so it does the public core include privately owned satellites or wired networks, antennas, devices. It's that also not clear.

And usually when we think of something being in the public sector it means it's owned by the government so again what does that imply this idea of public so I think for us the norm of protect being the availability of the Internet is a great I'm for a norm. But by introducing a term like the public core which is not well understood or difficult to define we may be causing more problems and it seemed like you were saying in your presentation

that first we agree the norm, and then after that we decide what the public core means and that I think I may be doing it the wrong way around. As I say we would support the aim and be keen to engage in this conversation but I think there are concerns here about how this concept of public core is understood and how might be actually unhelpful if had some ways. I will be interested to hear the panel's comments on that. Thank you.

MANAL ISMAIL, GAC CHAIR: Thank you. U.K. I have Argentina next.

ARGENTINA:

Thank you commissioners this is Olga Cavalli from the government of Argentina. Thank you for visiting us in the GAC I have some questions about the commission itself. As you have sponsor... and secretariat and partners and commissioners. How -- and I see you have some ministries from government. How a ministry or a government could support the work or sponsor the work which is the process. To support the commission and how the commissioners are selected if there is rotation. If there is some regional diversity balance or -- how are they selected or appointed. Thank you.

MANAL ISMAIL, GAC CHAIR: Thank you, Argentina. I have the CTU next please.

CTU: Thank you to the commission. This is Nigel Cassmire from the CTU. Following on from Argentina as following onto Argentina is our question. At I'm not clear as whose initiative is this commission. And what will happen to the out puts of the commission what is your hope or pecuniary takes for the out puts ever the commission and is there a strategy to encourage its acceptance ever implementation at various stakeholder levels. Thank you.

MANAL ISMAIL, GAC CHAIR: Thank you CTU. Indonesia.

INDONESIA: Thank you. I just wonder if you can identify the commission. Pie name is... from Indonesia. If you can identify which, where you put your mission as was reported then you give it to us. Compare with the other output of several other commissions because we have something like global commission on cyberspace. GCSC we have the one set up by CG and Chatham House on so on. Now I understand that they have not yet set up comprehensive view on the cyberspace but perhaps you can identify in which field you

would like to fill in the problem that we face in the cyberspace bearing in mind that we have the several others study like that. That's number 1.

Number 2 I like your comment because you would like -- you tell us what we can bring home of your results, and I think that is very important because I want to -- I need some feedback also about the stability of the cyberspace in Indonesia for example. At the moment, for example in the... if I want to talk about universities in Indonesia I will say, but I will use the reference of several information ranking of Indonesia and universities in the world of the same with economic Indonesia. I can use standard and poor index. Now is there something that you can tell us from the index point of view or studies view that okay you Mr. Ashwin, your .ID... is this is bad. This is good. This is fair in this field you are not good because of. Ba and then I say, oh, Mr. ministry -- that Mr. Hakeem said that we are not good because of this, but we are good because of this, so that I can know what I can improve so I can tell some universities how to improve and so -- thank you.

MANAL ISMAIL, GAC CHAIR: Thank you, Indonesia. I have one last request for the floor from Congo and then we will give the panel a chance to answer. So Congo, please.

DEMOCRATIC REPUBLIC OF CONGO: Thank you, chair. Blaise ... GAC representative from the democratic republic of Congo. Thank you for the presentation. I should have this was the very first time I have heard about this commission. And I really appreciate -- I mean the -- your business call what you're doing under namely the stability of the cyberspace, and as the colleague from the U.K. has just mentioned. This is a bit wide and it is -- it's I mean it's so complex, and I would like to nominee from the government perspective on which components, on which segment exactly you are targeting and providing or coming out norms and should have be cleared or explained clearly if it is a for interest because it might be for great interest for some governmental bodies or regulators and in your interaction was the bodies how do you... who comes you to, do you go proactively or the other side can come? I really need the commission members to explain on which sides on which parts components of the cyberspace you're really target to produce these kind of norms and maybe we can call the regulations and my last question would be maybe I was a bit -- I was not very careful when you were making the presentation, I would like just to know what is the are the proximity of the commission business global commission but I still see in your address the Netherlands. Are you based in Nederlands, or what

links the Netherlands to the global commission. Thank you very much.

WOLFGANG KLEINWAECHTER: Thank you very much. Alex will be more specific if it comes to the public call but let me just explain it a little bit the background. Being in this field since nearly 20 years it's an ongoing process of discussion and you have on committee panel. The next commission and very often it's a continuous process. And some people refer to the global commission on Internet governance which was chaired by Carl ... and which produced an outcome for a global compact and a number of commissioner from the BILDT commission are part of this commission. The commission came to a conclusion and the conclusion from the report was -- to be more specific and so far the global commission and stability in cyberspace is we have to go in particular in this field of cybersecurity.

These are the key issues and we have to be more specific what. Are the elements which enhance the stability of cyberspace, and and so for it's ongoing process and as I said in the beginning, you were contributing to process which we continue in various circles into the 2020 so just in September we did 2 U.N. groups debate about cybersecurity and our conclusions norms is an input into

this process. So there is never an end. Never a beginning. Never an end. It's ongoing process of discussion which keep us busy in the next 20 years. With with regard to the public core norm it's also work in progress. So that's why we were very interested and very thankful for the debate we had with the stability and advisory committee, or let's say with members of the committee. So to find out in a more detailed may you know what are the elements of the core, and so if you have some additional proposals from improved language so this is the right moment to deliver us so that we can be more precise. I think we have an understanding and Alex will go a little bit deeper probably you can go back to the slide. That we have all the 4 elements. And we all have the feeling that this is an issue the protection of the core of the Internet which is in the interest of all so it means regardless of the difficulties and conflict we have in cyberspace all sides agree that we should not attack core elements of the Internet, and if we are very precise then we can enhance the efficiency and effect of the of this norm but over to Alex probably you can see a little bit.

ALEX KLIMBURG: The question from Senegal first.

SPEAKER: Sorry, Manal, did you have a question?

MANAL ISMAIL, GAC CHAIR: We have a very last request for the floor from Senegal. So maybe we can take Senegal first and then continue with the answers owe Senegal please and please keep it brief us what we are over time.

SENEGAL: (Interpreter) The Senegal representatives speaking. We had many many questions but there is one particular question that has to do with the Internet stability, this is a key question, tan has to do with the establishment on contact points. We know that this question was addressed on many occasions but I would like to know what is your role in this regard, and how you can contribute to establishing contact points? We saw that when we had the attack to the ICANN system. The cacophony existing in terms of communication. Countries didn't know who to resort to so how do you contribute to having a better database if you will for contact points that might help us to preserve the cyberspace stability. Thank you.

MANAL ISMAIL, GAC CHAIR: Back to the panel. Is it Alex? Anriette.

ALEX KLIMBURG: First on the note of the public core I think I just a couple of comments. And I think the example from U.K. representative encapsulates how many different views there are of cyberspace including the ministries. When we refer to the term public core we are building on the use of the term global public good rather than a global public resource. And the term global public good is not only an academic term of art it's also a term kept in international law, and describing cyberspace as a global public good has been an EU position since 2010 so within that context there are people who could associate the term public in this case as an attempt to nationalize parts of the Internet. We haven't had that comment often because most people associate the elements of our work more clearly with very specific global public good definitions which are more of more comparable if you will even to the laws of -- law of the sea.

And within that context I think it does the opposite. What it actually does is that it basically establishes that parts of the Internet does not a global public resource but in parts of the Internet need to be protected from exploitation from all users. Not through essential organization which is a global public resource would imply. But through other arrangements between the actors concerned. The way we have defined the public core of the Internet from point 1 to point 4 and these are obviously just

the headlines there is certainly technical details that goes into each of those points. And which is based upon surveys done with different parts of the technical community in one particular survey that was run by the Woodcock clearing-house which -- the routing community these aspects for us go outward in terms of level of clearness so we are very clear on one and 2, and less clear of the others.

But to come back to the original question of why not have to fully defined before being rolled out, we have defined it as far as we thought it was practice particular an it will on do so within the amount of constituents and also on the understanding certain issues are further defined in implementation this is also the aspect of secondly law I referred to beforehand is some parts of these are clear cut. Some are less clear cut and how it's defined will depend large on you. I would like ask Anriette as well.

ANRIETTE ESTERHUYSEN: I wanted to address this. Alex you should respond it the questions about the commission and how the commission was constituted. You have a he covered most but I wanted to emphasize when we talk about the public core rear explicitly not talking about public as in government owned and controlled. We are using public in the sense of common. A common resource. And, in fact, that

comes at the heart of what the ICANN multistakeholder community is trying to do and does. Which is to bring different stakeholders together, to look at rules, operations fairness of the DNS. Which is part of that public core. It is not opened by government. It is not owned so totally by private sector. Different stakeholders groups are involved and have to be involved to ensure the stability and security and interoperability of that system and that is how we think of public. We know public means different things in different parts of the world so we can you know we can deal with that. And, and to the U.K. your question about infrastructure we often get that, why do we include the physical layer. Cables that are owned and laid by private companies, even satellites we don't mention them yet. The reason is because they are essential for the availability. If you are from a small island developing state and you have one cable. Or you're a land-locked country and you depend on one satellite link, or primarily on one satellite link. That might be privately-owned transmission infrastructure but if it's disrupted or attacked that's going to fundamentally affect the availability and integrity of the Internet which we see as a common resource.

So I know that's tricky but I think there's very important to understand that we see public here as meaning common. Not public as in owned and managed solely by governments. But of

course governments are key stakeholder group in that. And just quickly to the questions about Indonesia. And DRC we are not creating a ranking firstly. We are not ranking countries. We are not evaluating countries in terms of their security or stability strategy. We are trying to provide norms that could be useful at a national or a regional intergovernmental or at a multistakeholder level. So if you are selling a national security strategy or a broader stability strategy look at the numbers. They would be useful for you when you do your own policy development. And then I think finally just in terms of who else were you working with the one thing to note particularly for those in Africa. Our next meeting will be in ADASABBA(?) Hosted by the foreign commission. It will coincide with the forum on cyber -- another one of these body in the space much more or oriented towards capacity building. And therefore we think really important for us to collaborate with both the African union and global forum. Alex, I will let you answer all the others.

ALEX KLIMBURG:

Thank you, Anriette. I would like to just highlight the other questions that came and would like to invite the commissioners to jump in with additional comments. First regarding Argentina, for instance, how to support the process. How the commissioners were selected. How how can people would, with the commission

of the first aspect is system. He have we have no legitimacy. We are a self-selected civil society member of largely retired people but also some people were in academia and do other things. And we have just ways country come to act in the basis of our own wish to contribute according to the process that we think are useful.

The role of the management Board is very very passive. They do not provide steering on content. We do have indeed we have contradicted some of the stated positions one or two of our management Board members for instance so and that is actually clearly discernible if you look at the contend what we work and and what they work on. They have been decent partners about the process not about the output. We try our best to reach out and to all governments that respond to our general plea, please work together. We do that on different levels. Including starting at the very basic informal exchanges. And it goes all the way up to being hosted for some of our actual physical meetings. All of these are open to you. And please feel free to reach out in any way you like to the chairs directly, to the secretariat headed by myself, and most particularly to the commissioners who are people you tend to know. So that would be it than that. Anybody on the –

UNIDENTIFIED SPEAKER: Yeah, hosted in the Netherlands with the center for strategic studies.

UNIDENTIFIED SPEAKER: -- Hague center for strategic studies and [inaudible] in Washington. It was the Dutch government who gave the whole process a push. They hosted the HAGUE meeting and the Dutch government pushed for the global forum of cyber expertise. And so the idea after the end of the BUGE commission was cooked mainly within the Dutch government and then the Dutch government reached out to us as partners and the commission was formed. I expect after the end of this commission and the discussion will be produced by the report from the U.N. panel we will see another commission will take this work Board and continue the discussion into 2020's.

ANRIETTE ESTERHUYSEN: Anriette responding to Olga Cavalli Argentina's question about members and rotation. There's been a little bit of rotation. Just in the two, 2 and a half years we have exited to make sure we have existed to make sure we have better geographic representation. It's not perfect, but we feel strongly we they had needed to come to an end and we need to do what we've done. Give it to

yourselves and others. To work with to change and adapt. And fought to be we are not a standing commission and of any kind and as Wolfgang said there might be a need for different or similar types of processes in the future. Remember that timing of this commission is significant. We were launched in had the beginning of 2017 which was at a time when it felt like the multi-lateral system was not going to be effectively dealing with cyberstability and security issues. But now we are in a very positive time. We have the open-ended working group in the U.N. first committee. We have another round of group of governmental experts. So we feel actually the timing for us to finish our work is good.

WOLFGANG KLEINWAECHTER: One point for clarification, probably I was misunderstood. This is not a governmental an affairs. Governments were hem to contribute to this process which came out from the community.

ALEX KLIMBURG: The community started with 5 interested parties. Most of us were at Harvard at the time and went from there. To pick up also on the related question regarding what are the links with the other commission that is have done previous work and are cons excavating to this space. I this it's important question. The global commission Internet governance preceded us and in many ways

was also a model I we orientated ourselves to .. . Many of our commissioner were part of that work and we addressed one particular gaffe gap we think didn't spent a lot of time on and that was the gap regarding norms. Now norms what we work on norms there are sometimes a little hard to grasp outside of the international security or first committee bubble but effectively the sometimes addressed a soft law.

They are not legally binding but they are politically binding agreements but they being be used to clarify standing international law so one of the contribution of our work is that people can use our work to effectively help clarify existing international law but also international humanitarian law, law of armed conflict. Our norms apply in peace and war time. District... this is part of the intents. What we think we trying to capture. But also the question is how can governments in particular and countries get support from the global submission on how to rank or understand how the effort has been so far. I would like to ask Abdul-Hakeem Ajijola.

ABDUL-HAKEEM AJIJOLA: If I may quickly to the gentleman from Indonesia. We actually have developed a tool that includes a scorecard. It's not yet officially launched much it's still in BETA and if you don't mind

maybe at the end of the year maybe if I am able to come to BALI for the OICAGM I will look out for you and demonstrate at that time. To the gentlemen from Congo I would like to ask that there is definitely some of the norms that you need to look at as a regulator because the norms require your input and activity. 2 of them I would draw your attention on are the norm for the vulnerability equities process and the norm on basic cyber hygiene. I mean we can talk about this off line.

And then to my brother and colleague from Senegal, I think his observation we've taken notes of it. -- two quick things. Yes, we will consider it. But please understand that has been mentioned by other colleagues. We are in the sunset phase. We have no intention to perpetuate ourselves. We just want to kick start this process and frankly you know hand it over to people like you so that you use the parts that you think are relevant to you, and move the process forward. We are R we are simply an input mechanism to your own thinking and deliberations. Thank you.

MANAL ISMAIL, GAC CHAIR: So, thank you everyone, thank to commissioners and thank you for reaching out to us and thank you for this informative presentation and fruitful exchange and I do apologize to my GAC colleagues who were requesting the floor, but we are already

almost 20 minutes over time, so I do apologies. I hope we keep the channel open and we continue to provide hopefully useful input to your process. So thanks to all commissioners, and thanks to GAC completion and to GAC colleagues please be back in the room by 1:30 because we're meeting the universal acceptance steering committee. So thank you.

[END OF TRANSCRIPTION]