RAW FILE
WSIS FORUM 2018
MARCH 20, 2018
1645 P.M. CET
BUILDING CONFIDENCE AND SECURITY IN THE USE OF ICTS

Services Provided By:

Caption First, Inc.
P.O Box 3066
Monument, CO 80132
1-877-825-5234
+001-719-481-9835
Www.captionfirst.com

***



***

>> PAVAN DUGGAL: Hi good evening. Welcome to this session 7 this evening of the WSIS Forum 2018. We -- today we are going to discuss some very, very important topic, building confidence and security in use of ICTs. And we have a distinguished panel. The time is going to be of constraint. So as in other sessions we request our distinguished panelists to just speak for four minutes with additional 30 seconds for wind up because we want to get more of your questions, your view points and interaction with the panel. Because today the world is not just about ICT. About the confidence that we have in the ability and resilience and their security per se. But think what better way to start this entire session than to have a perspective from the ITU because we are at a very historic junction of point in time in history. Why? Because it is not just two important milestones but we are also doing some remarkable stuff. It has been ten years since the global ITU security has been launched. I want to call upon Ms. Doreen Bogdan-Martin from the ITU to give her perspectives on this entire issue before we can kick start the

discussion.

>> DOREEN BOGDAN-MARTIN: Thank you very much and good evening, Ladies and Gentlemen. Thank you so much for staying with us. It has been a long day. But we are ending here with a very important subject as you said and that is building confidence and security in the use of ICTs. So maybe before I look back to 2003 and where this started I would like to look ahead and look ahead to 2030, Agenda 2030 just 12 years ago. And what we heard today in all of the sessions is that we will not achieve the 17 Sustainable Development Goals unless we achieve creating an inclusive information society for all.

And in order to do that what we need to make sure that we have built a trusted safe and secure ICT world for all.

And now if I look back as you were saying Pavan to 2003 when world leaders gathered here in Geneva and they adopted the plan of action. One of the kill pillars in that roadmap was action line C5 and that's confidence and security in the use of ICTs. And ITU is giving the role of lead facilitator in that action line.

And then stakeholders came together in 2015 and did a review of the WSIS process and what they discovered was that building confidence and security continued to be an even bigger issue than it was in 2003 and that more needed to be done.

And so at the ITU side what we have done in role as lead facilitators we launched the global cybersecurity agenda. That lays out a legal framework for consideration, strategies, capacity building, as well as aspects of international cooperation. We at the ITU assist Member States in building certs in capacity building programs through our work in the development sector and we also do a number of activities in the work of our standardization sector. And if we are really as I said in the beginning going to achieve having an information society for all, we really must work together all stakeholders from governments to United Nations and the private sector to really achieve a safe and secure inclusive information society for all. Thank you.

>> PAVAN DUGGAL: Thank you for giving us that perspective and thank the ITU has played not just a thought leader. It has been an important catalyst in the entire growth and evolution of the process of the WSIS. And every year when we come for the WSIS Forum we find new discoveries, new talents and new opportunities and new knowledge and most significantly far more investors for the growth for the WSIS process with as a whole. I want to call on the next speaker. We have Her Excellency, the concerned speaker from Romania, Ms. Maria-Manuela Catrina who is the Secretary of State and information society. Excellency I have two questions for you. My two questions how do you see the

role of Governments and public authorities in building and in preserving a secure online environment. And No. 2, taking in to consideration the fast-paced developments of today's new technologies how can we prepare the new generation in facing these new kinds of challenges? Over to you.

>> MARIA-MANUELA CATRINA: Thank you very much. Thank you for the questions. Just for starting I must say that I am very happy to see many so women in the room. It is something that I always say this type of conferences because we work in a field where it is rare to have -- to not be the only women. I am confident here that it is more friendly. And if you speak of role of Government it is always in speaking about confidence and cybersecurity I think it is very important to work together. Because this is a field where none of us can be secure on behalf of less security of the others. We all are secure together. That means it is important to share information, to share concerns to work together in sharing regulation. In Romania we work a lot in implementing the least directive and enforce the role of such. In two directions and this means first of all, creating the excellence in cybersecurity because we believe this is a field that we are good at. Because we are good in math. And we have infrastructure of excellence centers, if it is academia, we have the -- the Civil Society academia and Government and security, security organization that works together. And on the other side getting to the next question to be brief we will give a lot in education. This means that we do two things. Starting from the fifth grade each Romanian student attends mandatory course in computer science or informatic and we change the curricula, very soon. That means that we prepare the next generation for secure online environment because only we as humans can make a decision that machines cannot. Today is the International Day of happiness and I cannot remember a day when Robert tell me it is happy. Even if I work a lot with Artificial Intelligence they say they are ready and prepared and they know the solution but they don't say they are happy. And this is I think something that we usually forget when we speak in this technical area. That we are still human and we are the humanity makes us happy and especially good day for us. Thank you.

>> PAVAN DUGGAL: Thank you. I am going to take you ore to India. We talk about happiness and you come from a land that 1.3 billion people up there. Clearly there are a huge number of challenges and we have one of the foremost thought leaders. Secretary in Minister of Department of Telecommunications Government of India. She has a trail blazer and has been responsible for transforming large number of electronic Government services. I have a couple of questions for you in

afternoon. Of course, these questions come out of the fact that the entire world is looking the at India. What are the challenges in the Indian context for ensuring a save and secure use of ICTs? The second question is what are the vary steps taken by India for building confidence in use of ICTs, especially financial transactions and what's the Indian roadmap in the coming future times in this regard? And finally, how can India contribute to the WSIS process in respect of a safe and secure use of ICTs and what Strategic Plans does India have in this regard?

>> Thanks. So regarding your first question I think it is safe to say that every country faces the challenge of cybersecurity but I think what we face in India is that this is a country that's amongst the leading digitizing nations. Where you have organic digitization happening countries have little more time and, you know, the necessary space to come up with, you know, their own cybersecurity architecture, rules, regulations. Now what happens when in a country, for example, in the digital payment space, I can tell you, when we had 300 million Indians taking to mobile banking in just the space of 6 months, so I mean that really poses certain unprecedented challenges because you have to build all your capabilities at one goal. You have to build the institutional cap ability and you have to build the operational capability. And at the individual level you have to make sure that the citizens have the capability to deal with this. Because at the end of the day they are the most vulnerable.

So in India we have tried to, you know, build this framework through several building blocks. And the first building block is the -- to have a good comprehensive cybersecurity policy which we developed and I think Pavan you played a role in this 2013. Today we are in process of attempting to develop our own cybersecurity law and I think I will go back to what Pavan said because this is where Forums like WSIS need to play a more proactive role because I think there is it no one country which can come up with best practices all on its own. So we need to aggregate best practices. The second we do have the framework in place for setting up sectoral CERTs and we hope that as far as the financial space is concerned we will have the first financial sector CERT in place maybe later this year. We are planning to follow it up with a telecom sector CERT. We are building a national center for cybersecurity coordination. This is a high-end capability that will allow us, you know, to deal with large metadata. And we are also by the way when we speak about security and confidence I think that data protection is also key. And so India is working on a forward looking data protection law. And at the operational level we do -- we are

working on three or four things. One is to ensure that the courage is secure. Your core telecom networks must be secure. Second content that flows on T the applications must be secure. And third the devices on which you access, you know, the data that has to be secure. So I think that very briefly is the broad architecture on which we are working. I think this is one area more than anything elsewhere we all really need to collaborate. And India for its part, you know, we have developed certain capabilities. We have a large number of startups which are working in, you know, cyber area. We also have legal entities that are working and so I think we would be happy to contribute whatever we can to the whole WSIS process.

>> PAVAN DUGGAL: Thank you for those perspectives. So clearly India represents a kind of a case study. When you are talking about this huge population, and you are talking about life changing game changing scenarios, clearly India is a power to watch as you go forward. On to the next speaker from Turkey. Dr. Omer. Communication technologies authority. Dr. Omer Faith Sayan. I have two questions. First what are Turkey's efforts to ensure user's confidence in use of ICTs. Can you explain what's your work In Turkey in this regard. How can we increase security and what would be Turkey's perspective in this regard. Over to you.

>> OMER FAITH SAYAN: Thank you, Mr. Chairman. The statistics in Turkey shows the user ship of ICTs has been rising. There is the regulatory of Turkey we have many activities regarding this. We have established a center, to increase awareness. Also we started to operate on Internet help line and safer website where families can kind advices for safe Internet. Besides we put safer Internet trade in to service to provide children and young people with (inaudible) where they can experience technology and to raise awareness on use of Internet. This we know that the fact that ensuring user's confidence in ICTs requires a close cooperation with many Actors as we signed agreements with the Ministry of Family, Ministry of Education and Ministry of Youth to support all families and especially our children so that they could become more conscious Internet users. For example, in collaboration with the Ministry of Education in Turkey we conducted training for trainers on safe user of ICTs and created distance education models through which more than 50,000 trainers have been trained. And these trainers train them 107,000 teachers approximately so far.

In addition to public agencies and NGOs we try to collaborate with private sector also. With the private sector company in Turkey we started a movement with the saying don't be a cyber bully. Our aim is to attract people's attention to this problem and protection of personal rights. I would like to mention all

stakeholders including global social media companies an and Internet Actors should work together. Our children, our people should not only see data and market, but also as social human beings. And security has always been an essential need for (inaudible). However today's security is not only related to the real world but also has become requirement in the cyber world. So to view cybersecurity as a part of national security because of the mix associated with the course of social and technological advance, three essential components for increasing to cybersecurity and technology are human resources and well defined processes. So we are on that. According to research reports 6 million cybersecurity employees will be needed in 2019 globally. We are aware of this and we opened up post programs at more than 20 universities on cybersecurity in Turkey. We established a national Computer Emergency Response Team, to carry out coordination at national level in order to fight against cyber attacks. Eight sectors sets have been established in addition to all Governmental and private sectors have established their sets. And we As Turkey would like to invite all national state s to work for in the international cooperation issues so we can increase security regarding use of the ICTs.

>> PAVAN DUGGAL: Thank you. Highlight of cybersecurity per se, the question everyone is asking is how can we come up with some norms of behavior in cyberspace. I in the last presentation cybersecurity will be the No. 1 priority for all nations. If you don't want to acknowledge it. No problem. Give yourself a couple of weeks and month and you will see how cybersecurity starts becoming the paramount factor which is going to give you a large perspective of Governmental. We realize there is no one international cyber law. So norms have to created. We at Microsoft which actually stated that there a need for Geneva digital Convention. There needs to be clarity on what could be the roles of various stakeholders as we go forward. But while that's being propagated we have yet another panelist today, somebody a close friend, actually from Stein Schjolberg who has done a lifetime of work in this space. And judge Stein Schjolberg has come up with a new idea and his ideas relate to a new Convention and in that context I am going to call upon you Stein Schjolberg. But I have two questions for you. No. 1 is a Geneva Convention Declaration for cyberspace at all necessary? And if so, what should be the basic ingredients and salient features that that need to go as an integral part of the such a declaration? Over to you.

>> STEIN SCHJOLBERG: Thank you Pavan. Cyberspace is a fifth summon space and legal measures among all nations. Dialogues and cooperation between Governments and norm the and

standards in cyberspace must be achieved through a United Nations framework. Regional and bilateral agreements may not be sufficient. More than 125 countries have until 2018 signed and/or ratified regional cybersecurity and cybercrime instruments. Have resulted in fragmentation and diversity at the international level. Global cyber attacks may constitute a threat to international peace and security and need a global framework to promote peace, security and justice, prevent conflict and main focus on cooperation among nations. Today the technological development of social media such as Google, face, book, Youtube and Twitter have been rapid and impact on society so fast that ethics and public sentiments have not kept pace. Conduct in social media need a better protection by cybersecurity and the law. I was a Chairman of the ITU high level expertise group of 100 experts from around the world established in 2007 and the Chairman's report in 2008 included also as follows: Cyberspace is borderless and cyber attacks can inflict damage in different countries in matter of minutes. Cyber threats are global problem and they need a global solution involving all stakeholders. Ten years have passed any more initiatives for a global solution. Why has the technological development not resulted in a global solution on the -- on United Nations level? Some law makers in the United States Congress two of them, had in 2016 admitted that they were calling for a Geneva Convention for cyberspace and stated we are setting ground rules that everyone agrees to abide by, a world where there are ground rules is a much safer world than a world where there is not. And you all remember Jorge Sorro's statement in January of this year, the Internet monopolies have the wills or protect society against the consequence of their action. That turns them in to menace and falls to the regulatory authorities to protect set against them. In the U.S. regulatory are not strong enough to stand up against political inference. The European Union is better situated because it doesn't have platform for giant the of his own.

And as Pavan told listen to bad speech from Microsoft and also listen to the monitor on cyber attacks. May 12, 2017 more than 300,000 computers in 150 countries and vital governmental and private sectors were affected. Cyber attacks have been shutting down critical infrastructures and crippling Government networks. The solution of buying problems on ads on face brook and Google on other social media with intentional harmful activities against other countries. Yes. Geneva Convention on cyberspace is needed. Cyberspace situation today may be a Geneva Declaration. Norms rules and standards may avoid fragmentation and diversity at the international level and be a global framework on cybersecurity. Standards in Geneva Declaration

should be discussed includes standards for international cybersecurity measures, standards for legal measures and standards to international coordination and cooperation on investigations serious global cybercrimes through Interpol, standards for global public and private partnership, through Interpol to establish partnerships with key stakeholders in the private sector. Standards for international criminal court or tribunal for cyberspace. I have a short conclusion. ITU is one of a leading organization of the United Nations system in coordinating international efforts on cybersecurity and should bring together all the United Nations organizations to discuss model guidelines on norms, rules and standards on the Geneva Declaration for sigh beer security. It may take one year, three years, or five years to finalize. Let me use this citation from the former U.S. President John F. Kennedy let us begin. Thank you very much. Dug does thank you. I am looking at watch. We still have time for some questions. I want to open up the session. Is there anyone in the audience who has any question? We have a hand there. This is Mr. Goyal.

>> NK GOYAL: Professor from India. I want to know is there a way that I am cybersecurity safe on my Internet or computer?

>> PAVAN DUGGAL: Great question. Let me first begin by giving a preamble. The first rule of cybersecurity that nobody is secure. Once you begin with the basic premise the thinking that we will be completely secure is completely Utopian thinking. Anyone in the panelist would like to take it. Over to you.

>> In turkey and human gains we like to show we have the harvest pack get for cyber -- so we should work hard and show that we are -- we have more different actions. So you can never say that any of us, always safe but we can show that we have heart for people.

>> PAVAN DUGGAL: Any other panelist?

>> Just a brief statement. I believe that we are in the moment that we spoke so much about awareness. We should move on in the position that we are also doing things. But each and every one of us participated in so many conferences. And also we speak about security as a -- by design, about products. We have as many products that have connected now on the IoTs. Remember the small memories are necessarily designed to be secure but also we should move to the security as a mind set because none of the asks to technically prevent by the device to be attacked. A person with a bad mindset can any time do something bad. So I think getting back, the first thing we have to do is teach our children how to live in this environment and be promoters of new environment to their parents. It is what we did essentially with other areas. Thank you.

>> PAVAN DUGGAL: I have been talking about the need for incorporating cybersecurity and cyber law as a part of school curriculum from the first standard onwards. Gone are the days that you study cybersecurity. You need to know what cybersecurity but you have something to add.

>> On the point on unawareness and what other panelists were saying before about the importance of people and the efforts that people can take to protect themselves. Tomorrow afternoon we have panel on child online protection. ITU with a number of partners and I recognize Salma in the back of the room who is on the matter of online child protection. We came together ten years ago. Awareness is absolutely essential in making us all secure and in particular our children. Thank you.

>> PAVAN DUGGAL: Thank you. I saw -- I see three hands. Okay. So let me first go there. And then we come to you and then to you. Over to you sir.

>> Thank you, Mr. Chairman. My name is Gavin. UK is not persuaded there is a case for a global cybersecurity. We think that it would take many years to create such an instrument and the time the effort and the energy are much better put in to measures which will actually deliver significant and meaningful benefit to users ICTs such as awareness building and training CERTs and exercising those CERTs. We should note there has been quite a lot of work done already in developing norms and CBMs. We note that the group of Government l experts has produced a set of norms governing the behavior the states in high cyberspace. OSCE has now agreed to two sets of cybersecurity building measures. Difficulties of coming to some kind of criminal court where the gathering and presenting of evidence will present immense technical and legal and political difficulties. We don't think this is somewhat beyond the reach of the mechanisms that we understand at the moment. Let us put our energies in to things which will help the world which will protect nations. A Treaty will not protect nations having good ge defenses and good and effective CERT will help nations and that's a much better way for us to go forward. Thank you.

>> PAVAN DUGGAL: We have that as a comment. Let's just -- small comment before I go on.

>> As we understand I disagree. Europe has around 47 members who ratified Council of Europe comments known on cybercrime. We are 197 countries around the world and other countries have other feelings and other conclusions than you are.

>> PAVAN DUGGAL: As they say it is a very complicated world. There are different perspectives in the spectrum and we must respect each of these spectrums while moving forward. Over to the next question. We had hand here, sir. Yourself?

>> Yes. Thank you. Being a lawyer for once I have to say I don't think the solution is in the legal field. That is really our technical field. I do a lot with cybersecurity. And realized that. Firms do not do their protection which they could do. For example, in the security operations center, as is service things like that, so know before -- you get attacked and at least in Switzerland and shocked how few have that. And if these things get done, and, of course, if you use the most modern software I think that's the thing that you can do. Because the legal situation is clear and it is a legal but first find out the hackers and how to prosecute. So I agree with what the colleague said before it is nice to have a big Treaty but I don't think the solution is there. One way you right awareness but do dimensions technical measures they are not cheap. But the costs when you get attacked are much higher.

>> PAVAN DUGGAL: So the costs are continuing to grow. 6 trillion U.S. dollars is the global cost on cybercrime by 2021. So clearly it is like different (inaudible) that go to the ocean. They take their own particular route of going to the ocean. That's a great perspective. Can I go on to the hand over there? Michael.

>> Thank you very much Mr. Chairman. Mike Nelson. I envy the Chairman of this panel half as many people as the last panel. We are having a real discussion. My question is about perception and misperception. Under like the previous speaker as a technology company I do believe that technology is the main answer to these problems and we have 80 or 90% of the technology we need to address the problem of Botnet attacks and cyber -- some of the cyber threats we are talking about. They just haven't been deployed and I don't think the law is the answer. It is motivating companies. They have to face the right problems. Point out one misperception that they would like to correct. I see at least two that every Day One is that everyone focuses on hackers breaking in the systems, and they don't pay enough attention to what can be done by attacking the system with bogus data and overwhelming website. And the second thing I hear a lot about is the need for cyber deterrents and somehow we are going to back hack when somebody attacks us we are going to attack them twice as hard. I don't think that's an answer either. Might be focused on half of the problem or the wrong problem I would appreciate hearing that.

>> PAVAN DUGGAL: Take the last question before I come for final comments with the panelists. Over to you.

>> I think I'm going to give another twist a question for the panelists, Doreen following up from our discussion at lunch I understand that my colleague has said from the UK this is an challenge and I remember how hard it was for us to get to see a

child online protection started. However as we promote more and more access to the Internet, we need to consider the naive the population with low literacy that are becoming vulnerable to threats from cybersecurity or lack of awareness. So technological solution is something that needs to be fast tracked through whichever body so that as we get more people in the rural community and Developing Countries with missing regulations and things in place how will we protect them. That's a question.

>> PAVAN DUGGAL: Fantastic. These are fantastic questions and go across the panel not just to answering perspective questions but coming up with final comments because I am told we want to wrap up.

>> Just I would like to mention that recent technological developments require change in cybersecurity which includes firstly reactive measures, cyber threats must be replaced by simple and cheaper actions. Controls and networks and infrastructure levels are needed besides system access controls. And third the users must be informed awareness level regarding the vulnerabilities and infrastructures and application systems must be increased and lastly, and the most important that we should also talk here the level of cooperation is great importance. So in other actions there are a lot of international cooperation but in cybersecurity domain I guess this is a bit your level. Thank you.

>> PAVAN DUGGAL: Your comments.

>> I think I would like to see much more being done in two areas. One is by the big technology companies themselves. And I think, you know, at least three speakers here spoke about the point that, you know, ultimately technology would probably have to do much more. You can have a perfect legal framework but, you know, if the technology has a lot of vulnerabilities I think, you know, the way to address it is through technology. So I think, you know, global companies particularly need to be asked to do much more. Rather than leaving it all to governments. Because I don't think, you know, Governments can do everything where we can't. The second area is particularly for given the fact that, you know, increasingly we are all focused on taking the Internet to the bottom of the pyramid and the bottom of the pyramid is really vulnerable. I mean in a country like India we are saying that digital is the way to empower people but at the same time if we expect them to kind of know how to use technology in a sophisticated manner I think it is really not possible. So I think globally we need to see much more resources going in to this area much more efforts going in to this area. So that the people who are most vulnerable need to be protect ed better. We need to spend more time thinking about how to do it.

>> Just getting back to technology issue, it is quite to do much more in technology and each and every company can do that but I will ask each and every one of when did you last update your home computer. Maybe the firmware update there but nobody really cares how about it. I would like more to see in the future the digital agenda is a social elevator for the less fortunate of us. And this means also investing in technology but also in education and about misperception, I think I'm afraid of having a cyber SMS next buzz word in each and every other discussion in that everyone speaks about football politics and cyber. Something should be left to the specialist and other part we should do awareness and we do a lot more in schools and with kids. Thank you.

>> PAVAN DUGGAL: Thank you.

>> DOREEN BOGDAN: Very quickly maybe to Mike's question about misperception. One feel that Governments alone are the solution and I think it has to be all stakeholders that we do need global cooperation and there is no one perfect solution to this -- to this great challenge. And in terms of Salma's point about the vulnerable groups and as we bring the next billion or last billion on line we need to come up with measures to protect. Awareness and protection of those vulnerable groups have to be front and center. Thank you.

>> PAVAN DUGGAL: Okay.

>> And this is it coming from the judge. Don't never forget that the main element in regulation on cybersecurity and criminal laws is a preventive element. It is very important that we give relation that prevent issues. And let me add also a wish in my prayers open up the excellent high level dialogue between United States and China in 2016. And include also Russia.

>> PAVAN DUGGAL: We can see that different panelists have got their own different perspectives. A lot of work needs to be done. We have done somewhat but far more work remains and different capacity building initiatives have to be encouraged in this regard. The international conference on cyber law, cybercrime that India hosts in November is one such initiative. That is also getting multi-disciplinary approach on how to deal with these challenges. There are questions but no one has got the correct answers. And searching those answers we have to put in our minds and our best intentions going forward. I want to disclose this conversation and this panel by referring to something that was written 5,000 years back. In the ancient scriptures of India one particular slogan. It says arise, awake, and stop not until such time that your goal is achieved. The goal for all us is very clear. We have to constantly keep on working towards finding effective solutions and thanks to WSIS Forum WSIS and also particularly ITU for giving us this platform

for us to discuss deliberate and push forward involving jurisprudence on cyber law and cybersecurity and it has been a pleasure and thank you to the audience despite the time ticking away you have all been here and listen to the fantastic discussion. Thank you again. We hope to see you in subsequent sessions as well. Thank you.

***



***