FINISHED FILE
WSIS - HIGH LEVEL SESSION 5
APRIL 9, 2019
1600 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

***

***

>> Good afternoon. Can we have the panelists down on the podium, please?

>> MORTEN MEYERHOFF: Good afternoon. Welcome to session 5. And particularly on the security angles of this. We have an exciting panel in front of us with representatives from both the public and the private sector. We are saving the best for last which is the two female additions to the panel. So it is not a male only dominance.

Just some house setting rules, I will introduce all the panelists in turn. We all have five minutes. Once the five minutes are up, a bell will ring and will keep on ringing until you finish off. We want to avoid any delays in the reception and people's evening plans, but we want to give you adequate time.

My name is Morten. And it is a pleasure to have you all here. I have already met a number of you. And the speaker order is

from our left side to the right or from your right to the left.

So we will start actually with a number of interesting panelists. We have the Deputy Minister of Information and Communications in Cuba. We have the State Secretary of Public Administration from Slovenia. We have got the high level board member from the communication electric posts. We have got the Chairman of the board of the ICT authorities of Turkey. We have the vice-president for policy at Symantec. We have the executive vice-president for the EastWest Institute. We have the director for strategy and innovation at the PANIAMOR Foundation. And we have the director of the Department of Telecommunications at the Indian Federal Government.

Lots of opinions and interesting programs. I will start straight away and ask the Deputy Minister of Cuba a simple question. What is the role of the state in creating confidence and security in people's use of ICT? And is it a pillar that we should address continuously or is it a one-off?

>> H.E. ERNESTO RODRIGUEZ HERNANDEZ: Thank you very much, Morten. I'd like to recall that in the Declaration of Principles approved by the Heads of State and Government in the initial phase, the world -- some of that Information Society it would follow stated, and I quote, "Put in place a climate of confidence in the security of information and network security authentication, privacy and protection of consumers is a prerequisite to make sure that the Development Information Society and to promote trust and confidence amongst the users of ICT", end of quote. This mandate today is gaining in importance in view of the fact that the use of information technology and communication ICT has transformed the Panorama of international security. In a number of different activities and white collar crime and different activities they go against peace and security. This has given rise to an increase in risks in recent years. When it comes to the use of ICTs for criminal purposes Governments must put in place different instruments and mechanisms and Treaties, cooperation agreements as well so that we can thwart these activities and has to be possible also to take these people to justice.

When there is an attack on technological resources and networks, the territory where the crime is perpetrated, it is logical that the sovereignty of states must remain fully fledged. They can give rise to international conflicts as well for the use and covert use by individuals, states and organizations to also attack the information systems of other countries. The only way forward as has been stated in a number of international fora in our countries, the only way to thwart this type of activity and make sure that cyberspace is not transformed in to a theater of criminal activity is cooperation

between all the states. And the ICTs once again should be used in order to further socioeconomic development, promote peace, knowledge, and eradicate poverty and social exclusion on the basis of the full respect of the UN charter and international law and not as an instrument to promote interventionism, wars, conflicts, subversion, unilateralism and also terrorist activities.

Notwithstanding today there is cyber terrorism there is a violation of privacy of people, fake news and hate speech as well. All of these are activities that make use of ICTs as well. And the accelerated emergence of new activities such as Artificial Intelligence, Internet of Things, 5G, mobile telephony and others is making the thwarting of these activities more difficult. More -- now more than ever before we have to strengthen the cooperation between Governments within the scope of the United Nations and with all the various interested parties as well in the appropriate fora to increase the trust of users and protect networks and data. These are the risks that we have. And in view of all of these we have to make sure that there is security of information and security also of the informatic networks.

>> MORTEN MEYERHOFF: Great start. I would like to invite the secretary in Slovenia to answer in this question. Children are often forgotten when we look at security and privacy. We tend to focus on the big picture. How do you work with different Nongovernmental Organizations, Civil Society, the private sector in Slovenia to protect children online and how you are utilizing, if you are, your regulatory framework in this regard.

>> H.E. LEON BEHIN: Thank you very much. And I apologize a little bit for being late. When we talk about Slovenia it is a small country in the European Union and our work together with (inaudible) and also Nongovernmental Organizations, we put something also in our regulation law. And also for the Nongovernmental Organization cooperation and also for the other things which is considered connected with financing. But we also think that the citizens should be able to learn about the risk of cyberspace and how to manage them and the associate responsibility to everyone for their own security in the global communication network. So for us it is our citizens, the main point also for our work. And we think there can be no good international operations but also Internet use without citizens and also with the trust of these citizens to Internet and also the Internet communication.

We must be able to be aware that citizens can still do the most for providing our own information privacy. To help raise awareness about security and communication privacy in cyberspace. We have several long-standing and successful

awareness programs in Slovenia. We give special phases to young people who will be future carriers of the digital transformation. Young people are the primary audience of a project within the safer Internet which we establish in the Government level. And in this safer Internet center we have three long-term projects, so-called safe point SI telephone and also in Slovenia we call split no code. This means Internet I. Safe SI is a point of awareness about the safe use of the Internet and mobile devices for the teenagers and parents and also for the teachers. Intense use of social network is video content, mobile application, materials for different age groups of young people, teachers and also for the parents. They carry out education through schools and also for the other institutes. And we have an organized support center which is already set as I said safer Internet center. Among the last project in the campaign, stop online violence against women and also for the girls.

This (inaudible) and it is an advisory line for online problems. Telephone on which between afternoon advisers answers questions, dilemmas and resolves your problems with using the Internet every day. The service is available for the children, also for the young people and their parents. And we established already in February 2013 so-called chat room which started in which is very good results of this, especially between the children, adolescents and parents. Internet online -- if you encourage and encounter such contact of the Internet you can report them on VIV. This is an Internet page split no code SI. Participation of similar points in Europe, fighting to reduce legal content on the Internet. The center of safer Internet is implemented by the University of Uganda and the institute, the Association for French. So this is the typical work between administrations and also with civil. And this center is financing to the European Commission and also for our Ministry of Public Administration.

Two strategies I would like to mention is about also the digital Slovenia which is implementing the UN directive. And we think that this kind of work in organization and also in collaboration with (inaudible) can do good results and also be better use for Internet in the future.

>> MORTEN MEYERHOFF: Thank you very much. A good example of staying on time but also hearing the bell. Be warned. I have the pleasure to ask the member of the French regulatory authority to join the conversation. Specifically I would like to hear how you are addressing the digital revolution in terms of the new type of services that people are now using. How do you as a regulatory authority address the issue of trust? How do you empower users, we are talking citizens and businesses to

maintain trust in authorities and in technology in particular when we have such rapid changes? So building on the previous speakers what is the regulatory response at France?

>> SERGE ABITEBOUL: So the first question we can ask is why is this lack of confidence of trust. And I think it comes originally from the ignorance in the new technology. As a member of ARCEP we have to go in to solutions that are more short terms. So first what we try to do is to encourage transparency and good practices, not surprisingly. We want to encourage also loyalty and fairness. So typically what we want is companies providing services to behave the way they say they do and should behave more properly. It is, of course, difficult when you defend this kind of position because there is also the freedom of speech that you have to support.

Practically what we do, for instance, is we provide measurement's performance and Net Neutrality measurements so that we can essentially tell users what they can do. We have done a lot of work on analysis and proposals for devices neutrality. When a user has access to the Internet through these services, it does it typically through a device. A device can be a telephone most of the time. It is a telephone. But more and more it is going to be a personal assistant, vocal assistant. The problem is that users cannot rechoose their device. The app stores sometimes limit their choices. The operating systems of the telephones also limit their choices. They provide preinstalled applications. All that is essentially preventing the user from freedom of choosing what the user wants to do. And this is actually accelerating with voice assistant we don't -- we have less and less choices. And I think this is bad for the users because it is talking to them like children. It is some kind of infantilization. What I want to insist on is really the idea that we should empower users as I said in the long term through education, but also in the short term by explaining what's going on.

The services should explain their choices, explain what they offer to the users in a cleaner way. Also giving back control to the user means that we want to encourage the participation of users. And there are many ways to do that. Not let the user be passive in front of the new technology but participate in it. So, for instance, we are doing some experiments with the crowdsourcing where the users are actually asked to provide a response or install some ads on the telephone to investigate the network, for instance. We also -- there -- that has been mentioned by previous speakers, participation by alerting when you find inappropriate data, for instance. Controlling of your data. There is a lot to do in the long term, in enforcing more and more interoperability between applications. This

interoperability we used to see in telecom. We find it normal with any kind of operator to call any other operator. If you move that to the Web services this is not the case. Because they try to capture you, they capture you. They capture your data and try to keep you inside a silo which again brings us back to what I said before, some form of infantilization of the user which really goes against what we want to do. We want to have generations of users that are empowered and again generation of users who will not only be passive users of this technology but active users. And that in a full circle is bringing us back to education. And I would like to mention a last dimension of the work of ARCEP which is data centric regulation. We believe that everyone should participate in the regulation, the companies that are providing the services, the users, the governments, of course, regulator, other companies. And all these should come by bringing in, putting on the table open data that everyone can check, verify and can be used to put together better services. Thank you for your attention.

>> MORTEN MEYERHOFF: Thank you. Very interesting combination of regulatory packages focusing really on trust. Moving on, I would like to ask the Chairman and President of the Information and Communications Technology Authority in Turkey what type of regulatory measures the Turkish authority is taking in order to ensure cybersecurity but also privacy online. And particularly examples of what you are doing in the Turkish context and how you are working with international partners in this regard.

>> OMER ABDULLAH KARAGOZOGLU: Thank you. It is on. Okay. Thank you. First I would like to express my sincere thanks for the opportunity and extend my gratitude to who have contributed to this organization. Diffusion of technology has led us to a new stage with respect to associated risks in the context of cybersecurity. Ensuring cybersecurity is not a -- also a prominent factor affecting nation's prosperity and national security.

Turkey's national cybersecurity strategy and action plan includes actions regarding strengthening cyber defense and protecting critical infrastructures, fighting against cybercrime, developing awareness and human resources, developing a cybersecurity ecosystem and integrating cybersecurity in to national security. In order to match the needs with respect to global skills shortage in cybersecurity we need to act quickly in this respect. We organize cybersecurity trainings for institutional CERTs from different critical sectors. We also carry out hands-on trainings and competitions for students and graduates in the last two years. About 2500 trainees have attended our training programs. And we also establish the cyber

in order to improve our training programs and provide more hands- on activities opportunities. We carry out early detection and alarms in terms of technological measures. We develop some detection and protection systems that play a huge role in the national cybersecurity by providing visibility, detecting command and control centers of Botnets and malicious software. Because cyberspace is a field, ensuring cybersecurity, a multi-stakeholder and interdisciplinary issue. We need to work with users, private sectors, national Government authorities, academia and international counterparts in order to fight against cyber threats. We believe that international standardization activities are also very important.

We take in to consideration the international information security and cybersecurity standards in our regulations for critical sectors. Sources and targets of cyber attacks may vary from country to country. Command and control center can be in a country while its target is another one. For this reason, information sharing plays a crucial role within this context. Turkey signed a cooperation agreement with the many countries. We also ratified Convention on cybercrime which covers various crimes including those committed via the Internet and other computer networks. All these cybercrimes are now incorporated within our national legislation.

Also Turkish criminal code covers unauthorized access to IT systems. Unauthorized interference, interception, modification disruption of IT systems. One of the main pillars of our efforts is developing a cooperative network at the national and international level. An organic network as we call it. Continue in substantial expansion of this organic network by making rapid information sharing among parties is multilaterally beneficial for all of our allies.

In the document published by the European Commission in April 2018 on measures to combat this information on the Internet, it is requested that global online platforms develop effective mechanisms for combatting this information. It is of great importance that states work in cooperation in this matter which is a global problem. All online platforms, especially media companies need to be responsible for false news. They need to provide ways to report this information more effectively. They also need to respect the decisions of judicial and administrative authorities. Of course, all these need to be done without prejudice of freedom of speech. I would like to finalize my words by fighting against terrorist organizations should be independent from religious and idolatry attached to these groups. Thank you very much for your attention.

>> MORTEN MEYERHOFF: Thank you very much. We are going to move rapidly on and look at it from a private sector

perspective. I would like to ask about cyber hygiene and education as you call it. And it seems that attacks no matter how secure we are the hackers seem to find a way around the latest firewalls. Do we need to educate our way out of the problem? And can machine learning and AI actually help us to safeguard our data and systems better?

>> JEFF GREENE: Thank you for the opportunity to be here. We appreciate it. I will take that in two parts. With respect to education and hygiene, the short answer is no, we cannot educate our way out of this problem. The longer answer is that yes, we can make significant improvements through education, through cyber hygiene. So what do I mean by that? It is simple things like not clicking on a bad link, watching out for suspicious e-mails, patching and updating your system. Using multi-factor or two factor authentication for your accounts. All those things will make the lives of the attackers difficult and drive up their cost of doing business. And if you think from the attacker's perspective they have a business model, too. And if you can make it more expensive and more difficult then you have had success. There are more complex parts of a targeted attack. You may see an individual e-mail targeted to you that may be spoofed, it may look like it is coming from your friend or spouse or boss. And you feel like you have to open it. But through education we can learn to be a little more careful.

At least in the U.S. and a lot of the events that I attend I hear people say that education doesn't work. And I think it comes down to how you measure success. If you are looking at it from the perspective of complete success, no, it doesn't work. But if you look at it from the perspective of improving the ecosystem having an impact it does. If 10 or 15% of the people learn to be more suspicious, we have made a measurement change. Education and hygiene frankly do work if you look at the history of the attacks we have seen.

Social engineering, trying to trick you in to doing things that you would never do if you were fully aware of the implications. We used to see attacks that pretend your computer was infected with pop-ups. Attackers had to move on in the public health sector. When we have had health emergencies we have taught people specific hygienic things to do in order to prevent spread of disease. If we look at it from that perspective it is wrong.

Switching to AI, if we look at how we use AI in here, I use the words AI, Artificial Intelligence and machine learning somewhat interchangeably. Ten years ago we primarily saw malware. Bad software doing bad things. It was not always easy to detect. But through evolution we and other security companies and countries have learned how to detect a lot of those attacks.

What we see a lot of today are the use of legitimate programs to do illegitimate things, good software doing bad things. Those can be much harder to detect. And they require analysis of a huge volume of data. Sometimes putting together two pieces of data or two things that seem to any human disconnected. They could be disconnected in time. They could be disconnected in terms of what they are doing on the computer, but we can use AI and machine learning to detect that activity to spot it and then present it to a human being to adjudicate it is something legitimate or attack that we need to detect. It is important regulators look at AI. And they understand the implications of ensuring that we and other security companies are able to use these tools because the bad guys are doing the same thing. They are using the same type of math, same algorithms to find ways around our protections. It is certainly an important role for governments around the world to spend, to look at AI and ML. But it is also important that you involve folks from the private sector and from my perspective from the security side so that we can provide input on how to best address this issue while at the same time making sure we can innovate and keep protecting as the attackers evolve. Thank you for the opportunity. I appreciate it.

>> MORTEN MEYERHOFF: Thank you very much. We move on to a foundation and the executive vice-president of the EastWest Institute. What is in your opinion the greatest threat to stability and security of the international cyberspace as we see it today? And what are the parties who are the parties that can address this most successfully? Is it a single party or something else?

>> BRUCE MCCONNELL: Thank you for inviting us here. The EastWest Institute works to resolve conflicts among states. And we do that in physical space. And we do that in cyberspace. Today we have heard some things about various malicious activity that is going on on the Internet that is using tools that we all use for good, for evil, whether it is for cybercrime, for stealing, for theft or also for more state-on-state attacks which effect critical infrastructure and have the danger of being part -- becoming weapons of war.

So the question is who is creating instability in cyberspace and what can we do about it. And what can Governments do about it and what can companies do about it because it takes both parties. So if you think about the larger point of the infrastructure, the -- what we call the public core of the Internet, in other words, everything that makes the Internet run, the routers, the routing system, the Internet numbering system, all -- software behind that, that has to work in order for all the things that we all have to do and depend on the

Internet to do our daily lives and do our daily work. What can be done about that? States have to exercise restraint. They have to not attack the public core. Now we can't imagine that states won't use cyber weapons. They will. They are very convenient weapons to use. They are inexpensive to use, but the key question here is should they in the use of cyber weapons take down the internet in a general way, in a large way with a mass effect. And the view certainly that has been proposed by a number of organizations, the UN group of Governmental experts, the global commission on the stability of cyberspace which is a multi-stakeholder group is no, that activity should not be conducted. And this is an area that definitely within the competence of study of the International Telecommunication Union because it is about the basic, the core infrastructure of telecommunications that the world depends on. So that's No. 1.

The second thing is that there is also a private sector angle to this and as all of you know, of course, the private sector is the primary owner and operator of the underlying infrastructure, telecommunications carriers, both international companies as well as national carriers, carry all the traffic, all packets, if you will, that we depend on in order to have communications.

What can the private sector do about this? Well, companies like Jeff's, of course, defend users so that when malware gets to you at your house or corporate gateway you can knock it down. But what if we were to go further down the stack and do it on a more wholesale basis? Today telecommunications companies already block Spam. They block at least half the traffic that's on the Internet is Spam. Telecommunications companies block that already. What if telecommunications companies blocked malware? What if they took all the signatures of malware that companies like Jeff's and others know about and just screen traffic for those purposes and blocked it? Why aren't they doing that today? There is two reasons. They haven't been told to do it and there is not necessarily a business advantage for them not to carry traffic. Governments have in their -- in their -- within their remit the ability to tell companies to block malicious traffic.

And the second reason and they do already, for example, with child infringing -- child exploitation content. The second reason is that they are afraid that their customers will sue them. They have liability because they are common carriers. They are supposed to carry the traffic. And so if you don't get your mail, and you suffer a loss you might sue the telecommunications companies.

So the second thing that Governments can do is to give them liability protection so that if they do block malicious traffic then they are not sued by customers. These are some concrete areas where the public and private sectors can work together to

stop the spread of malware and its usages either for criminal activities or for security activities that expand and hit critical infrastructure, and thus affects the civilian populations which is not the intent at all. Thank you very much.

>> MORTEN MEYERHOFF: Thank you. We have already heard a number of different panelists talk about the role of training programs, education, et cetera. So I would like to ask the director of strategy and innovation at the PANIAMOR Foundation, what is their role in building both confidence and enabling security when we talk about technology. Are there any hidden elements to success in your opinion or your experience?

>> MILENA GRILLO: Thank you very much for the invitation, the Ministry of Welfare and Social Inclusion and many other partners that have been working with us in this context. E-mentor Costa Rica is a confidence generating and safety generating for families and children that has become -- that was developed in a way that innovates public policy in Costa Rica. In 2010 the constitutional court in Costa Rica declared access to Internet as a fundamental right for all Costa Rica inhabitants. The Government expanded investment making of digital inclusion, a key national milestone both in terms of equal enjoyment of rights and as a means for personal, social and national well-being and well-becoming. The connected homes programming was launched in 2013 to tackle this challenge becoming the country's flagship initiative distinguished by the WSIS knowledge award in 2015. Slowly but surely the connected homes program developed as a connected program developed informed confidence in the use of ICT and child online safety emerged as missing pillars for tackling digital inclusion with underserved families. A segment of our society deserving and needing to become safe, responsible and productive consumers and proconsumers in the Information Society if the country is to own the SDG pledge not to leave anyone behind.

So here comes e-mentors. E-mentors has been a multi-stakeholder initiative from Day One with high level champions, Ministers mediating to secure formal Governmental engagement by main public entities with related mandates. Private ICT sector engaging in multiple ways, particularly through mentoring and volunteering. International cooperation, the global partnership to end violence against children accompanied the investment model by providing monitoring and funding. Providing valuable expert guidance and feedback.

Underserved families and children, the population target of this national program was recognized and enabled at all times as real makers of change, codevelopers of the model. Nonpartisan CSO PANIAMOR and providing evidence-based know-how and creating contents and methodology to generate informed confidence, not

any -- informed confidence to minimize risk and maximize potentials and documenting everything within and beyond the hostess program.

The strategy behind the strategy, hearing elements, e-mentors is a situated proposal. The national connected home program for digital inclusion of underserved families was determined and the host platform for installing capacity building. So they can go on and continue with it. It is disruptive. Usual but also very much so unusual stakeholders were credited and mobilize as essential enablers of sustainability and scale.

Cost effective, no new program was proposed to the interested party. But the development of a third component in to an already running national effort tackling digital inclusion, by providing connectivity and equipment by clearly missing what both evidence-based knowledge and the same program learning allow identifying as a central pillar for digital inclusion, informed confidence and security. Political but not partisan. That's also the key -- the core key. So there you have it. These are the codes and values behind e-mentors Costa Rica. I would like -- I wanted to take this opportunity to share what is really behind, you know, reaching a proposal that can alter a national policy and make it sustainable and scaleable. Thank you very much.

>> MORTEN MEYERHOFF: Thank you. Now we are almost at the end of our panel. So I would like to invite the last panelist, director of the Department of Telecommunications in New Delhi. So the federal organization to highlight some of the steps that have been taken in India to improve the confidence of use in ICT across the vastly different cultures and socioeconomic groups. One of the main challenges you have faced and how have you overcome them?

>> Thank you. First of all, I would like to express my sincere gratitude for this opportunity. It is indeed a privilege and honor to be part of WSIS 2019.

Coming to the question, as we all know that ICT has been recognized as one of the most important tools that we can have to achieve Sustainable Development Goals. And however we are also aware of the fact that we can harness the total potential of ICTs only when people are ready to use it and they have confidence in using ICT. So the Government of India is taking many steps in building confidence in its citizens. And I would like to highlight a few of the steps. I would like to share as we all know India's own developed digital identity technology which is known in India as Aadhaar. This has actually provided linking of Government schemes, delivery of Government services to the masses very effectively and efficiently.

One example which I would share is the scheme of financial

inclusion. And this is one of the biggest financial inclusion schemes across the world. And under this scheme which we know as Genhun, approximately 300 million people they have been enrolled with bank accounts. And this is a great step towards financial inclusion. And here around 83% of these accounts are Aadhaar. They are linked with the national identity.

And another thing which I would like to share is that 59% of these account holders are actually women. So this is very inclusive. So this Trinity of initiatives which we call as JAM, this has made possible to generate confidence in the citizens. It has made it possible for the Government to directly provide the benefits to the beneficiaries under direct benefit transfer. And it has resulted in huge savings of public money which is taxpayer's money and approximately 50 billion dollars have been saved through the use of this (inaudible).

We also know that awareness is one of the key -- you can say key points to ensure that there is confidence in the masses in use of ICT. And to generate that awareness the Ministry of Home Affairs in the Government of India has issued civil guidelines and keeps on issuing guidelines on cybersecurity and secure use of cyberspace. And we have a national cybersecurity policy which is -- which just to provide a safe and secure cyberspace to Indian citizens. As far as the challenges are concerned the traditional challenge that we have as you have already said that to take any initiative to design it for such a huge population which is spread across such diverse geographical and economic conditions, that itself is a challenge. And particularly for any technological development for use of ICT, the challenges is to provide that safety and security to a common citizen who may not be very tech savvy.

So the Government of India has already started a certain Computer Emergency Response Team. And this CERT is responsible for the incident responses, analysis and forecasts and alerts on cybersecurity issues and breaches.

And another challenge is to establish central equipment identity register that there is a unique identification of all the mobile devices. So on that also the Government of India is working. Apart from awareness skill is also required for the common masses in rural India to use ICT. So various schemes under the skill development are also being carried out by the Government of India in this regard. Thank you.

>> MORTEN MEYERHOFF: Thank you very much. As we started with a Government official, we finish with a Government official via both the private sector and NGOs and Civil Society organizations. Before closing, I would like to invite Mr. Preetam Maloor, who is the WSIS Action Line facilitator on this section to highlight what is your key take-away from all

these different presentations?

>> PREETAM MALOOR: So the key take-away is not partnerships. It is not a surprise, but that's something that should be our mantra. That's going to be key in building confidence and trust in the use of ICTs. And we have many organizations, many stakeholders who do fantastic stuff. And what we -- is to kind of bring the different stakeholders together to do impactful work. For example, helping countries setting up their national CERTs or defining their national strategy. Defining, creating and deploying international standards on security. Helping, protecting children online. Building human capacity. In every area we rely on partnerships. And that should be the key take-away.

>> MORTEN MEYERHOFF: You just saved me from spending time on summarizing. So thank you for that. Thank you to all of the panelists. Please give them a round of applause.

(Applause.)

>> MORTEN MEYERHOFF: And I believe that we are ready to set up for the WSIS award ceremony, correct? So there might be a short intermission, but please stay close by. Thank you once again to the audience. Thank you to the panelists. Have a nice afternoon.

***

***