HIGH-LEVEL DIALOGUE

HOGH-LEVEL DIALOGUES

HLD2 Enabling a Trusted Connected World (International Telecommunication Union – ITU)

Wednesday 4 May 15:00 – 16:30

CICG, Room 1

Interpretation A/C/E/F/R/S

Captioning

RAW COPY

Services Provided By:
Caption First, Inc.
P.O. Box 3066
Monument, CO 80132
1-877-825-5234
+001-719-482-9835
www.captionfirst.com

***

This text is being provided in a realtime format. Communication Access Realtime Translation (CART) or captioning are provided in order to facilitate communication accessibility and may not be a totally verbatim record of the proceedings.

***.

>> MODERATOR: Good afternoon, everybody. I believe we are going to start in about two minutes. I would like to invite the panelists up on the stage. As I said, we will begin in two minutes.

(Standing by.)

>> MODERATOR: Great. Thank you. I think we will begin the session. Welcome to this high level dialogue entitled Enabling a Trusted Connected World. My name is Kim Andreasson. I am representing duke advisory, a private consult tansy and I will serve as moderator. I don't think I have to tell you about the importance of the topic. Let me provide some context in 30 seconds. Between 2000 and 2015, Internet penetration grew seven fold from 6.5 percent to 43 percent.

Internet use continues to grow steadily through fixed and rapid adoption of mobile broadband. However, statistics also show that more needs to be done. 4 billion people from Developing Countries remain offline often in rural and remote areas.

As we tackle the digital devices it is essential but we need targeted policies and effective regulations to make broadband with emphasis on trust and security.

Given the many challenges in these different areas I'm pleased to have such an esteemed and diverse panel consisting of policymakers, representatives from private, intergovernmental and Civil Society sectors to discuss the intersection of capacity building, building confidence and security in the use of ICTs and enabling environment.

And with that, I would like to hand it over to the director of the telecommunications standardisation Bureau here at the ITU, Dr. Chaesub Lee to provide some opening remarks. Please, Dr. Lee.

>> CHAESUB LEE: Yes, thank you very much. On behalf of Secretary General, I want want to give a very warm welcome to all of you for the high level discussions to explore how we can enable this trusted, connected world. It might be this subject is a little bit strange because something trusted, is combined with a connected world. I believe this is one of the challenges and objectives for all of us. We expect over these sessions we can discuss how we can enable our Information Society, to convey the meaning of this trust. We have a good panelist. We will collect the views of the experts in this

session and find out how to move forward into the IQ activities. I'm excited to listen and I hope you enjoy this session. Thank you very much.

>> KIM ANDREASSON: Thank you, Dr. Lee, for that excellent introductory remarks. I have a very basic question to start off the panel. It is the same question for all of the panelists. The question is as follows: In your opinion, what is your vision for a trusted, connected world? And why do you see it as a necessity for implementation of the sustainable development goals?

And I would like first to ask the minister, the national Secretariat of telecommunications in Paraguay, His Excellency, David Ocampos, to go first. Please, Your Excellency.

>> DAVID OCAMPOS: Good afternoon. The focus on trusted reliable networks has two different aspects. Firstly, the human aspect. Secondly, the network aspect. And we need a multistakeholder approach, just as we have with governance because on one hand we have end users. On the other hand we have industry. And the government needs to take a role. The government takes a role in the form of regulation and laws. They are important firstly to bring new areas to the legal framework as they merge. And incident response teams need to be built into that as well.

Campaigns are also key because on the citizen side, on the end user side the biggest problem with insecurity relates to education. And the best antidote to this education problem and the thing that has the biggest impact is campaigns. We wield those campaigns jointly with nongovernmental organisations and the media. The role of businesses is very key as well in this ecosystem of cybersecurity because we can see that beyond the fact that businesses have specialists and so on and so forth, we still need massive budgets to be able to ensure that networks are safe. Without any doubt, in this fight against cyber crime we find what is almost a disloyal fight that has to be fought. We have, we rarely have 100 percent security in our systems. Yet we spend massive amounts of money on them. Yet one single individual can come along

and hack into these networks in various points around the world.

So we need collaboration between incident response teams for cyber crime, and that's a good practice that is generated a good deal of positive results where prevention and protection are concerned.

In every country we need cohesion. In Paraguay we are trying to ensure that those coherence across the system because the government can't do everything. Governments can establish policies, but we also have to bring to the table all those different players that don't always want to share information such as mobile network operators, the financial sector, the financial sector is always very keen to hide vulnerability where cybersecurity is concerned. But we need to bring them to the table.

And in legal terms, one of the matters which I think comes up a lot in different countries relates to prosecution for cyber crime. Metadata aren't always available for ISPs, for operators, because when we put this into a plan that is open to all, we often find ourselves dealing with something that pertains to human rights and the right to privacy, and so on and so forth. And many times those rights undermine our ability to prosecute offenders. Sometimes all we're trying to do is stall metadata, that we have basic information. It is not personal information, but even that is altered.

We need this to be addressed and I think we need a multistakeholder approach.

>> KIM ANDREASSON: Terrific. Thank you very much, Ocampos forgetting us off to the same start. Dr. Lee, what is your vision for a trusted, connected world?

>> CHAESUB LEE: Thank you very much. Let me start with a little bit of practical part because as we have talked we are living in an Information Society. This is a very vulnerable part.

To live in this society, from my memory, after we adopted IP technology in the middle of the 1990s, we had a lot of effort

to provide quality. Afterwards, broadband should be one of the issues, as to the quality of the Internet. And afterwards we had a lot of effort to make a safer Information Society that was a security subject. We did many efforts of this make safe Information Society with security concepts.

But still there are some problems. What is our level of credit of our living society? How can we credit our devices, even now many fake devices, stolen devices, unauthorized devices moving around.

A little bit more high level, how can we issue these data, is it multi-state in let me ask you, when you have partners with any new subject, one is easily a website and correct the contents from the website. What is your credit of this information? You collect from the website? This is good enough? As a professional? I bring up this as a report, how we can issue this, is it good enough as credit?

Now we are moving from Information Society to the knowledge society. As we recognize data from data, which defines the information. Based on this information, we can cover with the level of this knowledge. Even the data, is it vulnerable? The building of the knowledge society on top of this is a really reasonable way. That is, I believe, some concerns raised rather than knowledge. Even we are continuing with this making safe Information Society, but now many more are carefully watching how it can be a trusted society.

It could be in this regard, if the rationale is there is enough, I believe that trusted, connected world, we need trusted information infrastructure. That subject would be very interesting moment to prepare for the future. So in this regard I am very much interested in this session because now we are challenging our ideas about the trusted, connected world. We need trusted entities on top of this connected environment. I am interested in looking at this as we move forward.

>> KIM ANDREASSON: Thank you very much, Dr. Lee. That's a terrific addition, giving your perspective.

We are moving on to Mr. Richard Samans, a member of the managing board at the World Economic Forum. Please, Mr. Samans.

>> RICHARD SAMANS: Thank you and good afternoon to everybody. Not to try to give a comprehensive answer but maybe build on what has been said, and add a couple of points. The noun in the title here is connected. So maybe that is a good place to start. We all know and certainly this institution is aware and does a lot of work on trying to expand connectedness. Bringing more of the citizens around the world online. It is still a large challenge, a lot of progress has been made as our moderator summarized in his opening remarks.

But it gets somewhat harder as you go, it seems to me. As we try to tackle more and more of the remote and poorer parts of the world, it requires additional effort and creativity. And indeed I would say thinking through how one melds resources, blends resources. I would say that's a big part of any vision or any effort to try to fulfill a vision of a more trusted and connected world. How do we crack the lack of connectivity in many parts of the world, particularly in Developing Countries by bringing together the right frameworks on the regulatory side but mobilizing efficiently as possible all of the resources that are available, which inEably has to go beyond the public sector. One needs balance there.

Another challenge to connectedness is even for those who have access and have the underlying infrastructure is in thinking through this tension, if I can call it that, between maintaining the requisite degree of interoperability of flow of information and data, which is fundamental for people realizing the full economic and human potential that the Internet provides on the one hand. On the other side of the tension is giving a requisite degree of policy autonomy for sovereign states or subunits of government, as the case may be.

In respect of legitimate social concerns, cultural concerns, security concerns, and otherwise. This is fundamentally a connectedness issue because if we don't get that right and

we've seen evidence that in some areas we are not getting it right, then that core interoperability, that flow of data is challenged. And even though the infrastructure, one is connected in a technical sense by infrastructure, one is not really fully connected if you are not able to access the information you want; if you are not able to realize the economic opportunities that are there by the shrinking of distance and time that the Internet affords. This is a central dilemma. I think everybody here knows that. But it requires moving beyond the diagnosis of the problem, the characterization of it, and the initial reaction to it, which sometimes can be more about a debate and rhetoric than it is about trying to segment, breakdown the problem and figure out where the common ground may lie and what models are available that might inform governments and citizens as to what might be some sensible trade-offs there. How does one reconcile? That's the next stage of the process I think for the international community and for discussions like this here and we are trying to think it through and see how our platform can contribute in that regard as well.

It is not a black and Whyte issue, I find. It really is about thinking through the continuum of allowing a reasonable degree of policy autonomy and respecting that on the one hand, but also recognizing that if you tip the scales too far in the other direction we lose a central part of connectedness.

The last thing on what I've just described also that influences the trust. If there's better coalescing around models that strike a reasonable balance as perceived by Polities there will be not only assurance of connectedness but a degree of trust that is enhanced. Right now because we are a little bit in the wild west on this and in a little bit of in some case Polemical debate about it, we have a reversal of trust. It's incumbent on everybody of good will to sit down and piece through the different pathways. I don't by any stretch of the imagination think that there is a unique universally applicable pathway or trade-off here. To enhance trust, that thought process has to go.

The last comment here, third point I want to make is related to trust in particular. And that is a transparency of rules. Whether you are talking about the public policy rules on the one hand, and again like I say, different governments will probably end up making different trade-offs and choices, but the fundamental thing is to enable the stakeholders to understand in a transparent way how those choices were made and how the process to help engage and arrive at those decisions, but at least as important if not more important is once that framework is set, being transparent about what it is for everybody. That is necessary for trust.

And the same thing on the private side. For private sector policies that impinge upon these same issues, the handling of data and the like. Again there will be different choices made by different actors. This is a very distributed ecosystem we are talking about here. But for the trust in the system as a whole that everybody has a steak in, I think the most -- has a stake in, I think the most common obligation ought to be to be transparent about what those rules are in as comprehensible and user friendly way as possible. Because as we know, there is process transparency, there is pro forma transparency on the one hand and thoughtful transparency where you are putting yourself in the shoes of the consumer and therefore trying to make it as comprehensible and digestible and as decision-friendly as possible.

Those would be the three thoughts. Coverage and domestic content, I should say, one. Two, balancing policy autonomy with a global interoperability and flow of information and data. And three, transparency. Thank you.

>> KIM ANDREASSON: Thank you very much, Mr. Samans, for an excellent addition to the two previous remarks. We are moving to the next panelist. And she is Ms. Anriette Esterhuysen, Executive Director for association of progressive communications. Ms. Esterhuysen, please?

>> ANRIETTE ESTERHUYSEN: Thank you. You asked us what our vision is. I'm going to be visionary and also comment on the perspective not just of the Internet but of the more world

goal. I think we need protection of rights online and offline. Not just political rights but also social and economic rights. And this involves governments firstly not violating rights, which is something we are not achieving yet. Also governments playing their role in making sure that corporations don't violate rights. But I think it also requires people believing they have rights, knowing they have those rights and demanding those rights, in relation to their states, in relation to other states and also to corporations.

I think this is obviously also involves security. I think what we need is a notion of an Internet that is secure and stable being one which does thought contradict an Internet on which rights are protected. Also that security and stability is as relevant to individual users to financial transactions, as it is to national security. I think hain of our current discussions about how to achieve security and make policy around security on the Internet is preoccupied with the security of states rather than with the security of users and of transactions that take place over the Internet.

Secondly, I think we need greater social equality and inclusion. Access has increased vastly. And that can have an empowerment effect. On its own, access is not enough. That is why we are linking this discussion to the sustainable development goals. And how do you achieve less social injustice and more equality? These are not absolute. But it needs to be respected at a policy level. There needs to be efforts to challenge particular problems such as patriarchy and gender exclusion and to reduce inequality at those particular levels. It needs job creation, poverty reduction. An equality approach is the only way.

Finally, I think it needs peace. We live in a world where so much of the potential of technology and connectedness is undermined by the fact that wars and conflict continue. And people are desperate when they migrate or leave their homes, either for reason of avoiding war or because there is just no economic opportunity. Then that causes instability in other parts of the world which is not proving very effective at dealing with that. To me that really contradicts the

fundamental premise of the connectedness that the Internet and technology allows us to achieve. But it also needs to be connected at other level, global cooperation, cooperation between states and support for those that are the most excluded and most marginnized. I'll come back to mechanisms later.

>> KIM ANDREASSON: Thank you very much, Mrs. Esterhuysen for adding interesting points to the discussion.

Last but certainly not least, I would like to hear a viewpoint from the private sector. We have been talking a lot about public private cooperation and multistakeholder engagement. Welcome Mr. Withouter van Tol. He is the director of sustainability and citizenship at Samsung. Mr. Van Tol, please.

>> WOUTER VAN TOL: Okay, thank you. First of all, can I thank the ITU for inviting us to speak here today. It is a great honor for Samsung electronics to be invited.

I want to give you a little bit of background. Otherwise my answer to the question that Mr. Drey send asked us -- Andreasson doesn't make sense. Let me start here. Samsung electronics has a huge programme around the world. We call it citizenship. It is basically creating a win-win between the company and society. It focuses in particular on education, digital education.

Now, I am responsible for the European part of that. That's why I'll talk about that specifically today to answer the question. So in Europe there are 5 million young people unemployed. That's about 20 percent of the total, which is a huge issue for the long-term. Underlying that is a skills gap. So young people do complete education, but they don't necessarily have the skills to get a job.

And these are especially digital skills. There is a million vacancies in the ICT sector at the moment in Europe, but young people can't fill them because of the skills gap.

So our programme, our digital skills programme which is in 28 countries in Europe, reaches, has so far reached about two and

a half or three years reached about 100,000 young people between the ages of 6 and 24. Really wide range. With software, hardware, and all kinds of other skills that we've delivered there.

This all fits into the SDG number 4, of course, quality education.

Now, to come back to the question because I think this background was necessary, so a vision of trusted and connected society. So let's first focus on the vision of trust. I think the previous speakers have already spoken very eloquently on data security and privacy. I don't really think I can add much to what they've said. What I do think is after several years of working on this there's also a need to trust young people to have a full place at the negotiation table and to also get real responsibility so that we don't just give, but that they are part of the stakeholders, part of the multistakeholder approach.

Because that experience, the successes and failures are perhaps the best learning experience for their future.

Secondly, trust is also about enabling cooperation between business in our case and education institutions, government, and again young people. That trust is something that is earned over a longer period of time, but I can go in a bit more detail later on but certainly we have learned that trust and cooperation takes some time to develop, but are essential to this society that we are talking about.

>> KIM ANDREASSON: Terrific. Thank you very much, Mr. Van Tol, for adding an interesting perspective.

I wanted to ask a follow-up question of all the panelists. I think we will go in the same order that we did in the first round. That is basically a lot of you talked about the key elements for an enabling trusted world. I wanted to ask more specifically how far are we from achieving this? What would be your recommendation for what needs to be done in the short, medium, and long-term to achieve the enabled, trusted,

connected world? So would Your Excellency Ocampos, would you please like to start?

>> DAVID OCAMPOS: Well, certainly as regards consumers, citizens, and as the previous speaker rightly said the issue of education is a low process. Perhaps we start out with some digital natives, so to speak, who have some idea of programming as provided in education. But today anyone can fall prey to Phishing or get a virus on their machine. This necessarily will mean that we need to empower ourselves with best practices in terms of security. Without a doubt in the world of business there is a need to recognize that 100 percent safe business has often made the decision to adopt certification. But these are decisions which are not yet part of the routine of big corporations who have important databases or who manage critical operations.

But relating to the government, I would say that often you have to bring people to the table who normally would not sit around the same table. That's a good reason why we as governments might come up with a national cybersecurity plan, digital security plan.

There are lots of instruments that we don't use or nt been very widely circulated, as in the -- but some have. As in the case of a digital signature. But these are processes which are still in some cases prototypes.

>> KIM ANDREASSON: Thank you very much, Your Excellency Ocampos.

Moving on again, same order. Please? Chaesub Lee?

>> CHAESUB LEE: Yes, I have questions from a purely technical part because I am a technical engineer, especially as it relates to ICT.

It is a very good time to seek trusted, connected. Could be where we place the subject of our future of development. Just to remind you again, beginning of the 1990s we didn't talk about quality at all. But even in the middle of the 1990s we didn't talk about security. Those are two words, quality is

coming to us and security is coming to us. Now recently privacy comes to us.

So this would be a good time to be asking to the technical industry to think over how we can enable trust for the use of these ICT, infrastructures, services, and applications. Because enabling trusted connected world should be supported by those technologies as we now do with the SPT subject. We have many challenges, but now our world is quite good stage to say still, we have a lot of challenges, but because of getting some support from technologies, we reach a certain level.

One of the other reasons why I think about it that way is our working land, living space is increased recently, especially the cyber space. The physical space is relatively easy to manage ourselves. Any individual has a certain capabilities to manage, make trust of their physical things, physical environment. And now everything is connected like ITU, so easily. Anything is connected, then should be pure in the cyber space. But it us our ability, as professionals. Any individual citizens, their ability to manage this cyber space is very limited now. But our life is more dependent on cyber space, the economy scale is on the cyber space is vastly increased, very quickly. How can we wrestle with this? It could be a good subject. We can challenge the industry, we could encourage the industry to challenge how we can bring all these trusted, connectivity while ensuring this matter with the flow of information, ensuring this interoperability, and mobile platforms. If we have good capabilities, it could be supported policies, autonomy as well, I believe. Certain benefits we will get. So as a technical engineer I'm thinking it would be a good subject. We may challenge how we can bring about this connected, trusted connected infrastructure. It will be an important subject for preparing our next generation society called knowledge society. So I wish to challenge in these directions. It could be our vision for the future. Thank you.

>> KIM ANDREASSON: Terrific. Thank you, Dr. Lee. Mr. Samans, same question to you.

>> RICHARD SAMANS: I would pick up on the last comments. It is a fair and appropriate challenge. There are technical solutions, so to speak, quote-unquote, that would help with a number of these trust and connection dilemmas and challenges we are facing. So having an explicit invitation for a wide ranging process, process may sound too organised, but a dynamic in which companies are invited to dig in and dialogue and cooperate and bring forward possible technical suggestions. I wouldn't restrict it to companies. I think there's a heck of a lot of technical expertise out there in academia, Civil Society, technical institutions and the like. Some of them are in private sector, some have come out. There's coders. There's a rich ecosystem of people who probably have concrete notions. And I think it would be a very healthy thing if the political dialogue, which we have seen over the years in settings like this, becomes, if I understand what you are suggesting correctly, also a bit of a multistakeholder technical dialogue focusing on specific areas where you're putting out a call for some collaboration on some technical contributions. I don't think anyone is suggesting there will be silver bullets here, but the ingenuity of the crowd, if you will, is not to be underestimated.

And back to your question generally, how far are we? Well, I think we are quite far from many aspects discussed today of having a high degree of trust and connection. So I think it is incumbent upon all those who engage in these kinds of discussions who share roughly the same kind of aspiration to think about how their platforms or networks, institutions could contribute. We are certainly doing that in our future of the Internet initiative which is an attempt to use our particular platform, which is one among many, but it has some special characteristics, to encourage very concrete cooperation on different pieces of these puzzles.

On the security side, on some of the policy issues we are talking about here, how can we help provide out of process of engagement, dialogue, some clear guidance, what I was talking about earlier. What are some good policy typologies that

appear to strike a reasonable balance, and a few of these dimensions.

We are trying to again use our platform. We have quite a bit of experience in catalyzing multicompany public-private and Civil Society partnerships in Developing Countries to try to use that to good effect in certain geographies to expand the mobilization of resources and investment to help with connectivity. And I would add domestic national local language content and the like, et cetera.

So I think it is a good challenge you've put forward here. And I would just echo it and thought I would dig down a little bit deeper on that.

Let me stop there.

>> KIM ANDREASSON: Terrific. Thank you, Mr. Samans. We will move on to the next panelist, Mrs. Esterhuysen, please. Dreet dreet so what do we need to do? I think we need data. I do think we need research. We need analysis. We are dealing with the access gaps or security issues. I think we often in our WSIS Internet world talk based on assumptions or impressions. I think if you are going to really connect the world, you need to understand exactly where the disconnections are. Who are the people that are not connected. What are the primary reasons for them not being connected? Does it lie in the ICT sector or context or are there other social and economic factors that produce that?

I think evidence based policy and regulation is not a new idea, but it remains a very relevant idea. It is challenging in a very rapidly changing environment such as the one that we are talking about, but I think that's can be addressed by the sectors that produce and analyze data. Secondly we need to move away from the dichotomous approach, do you regulator don't you regulate? We wasted an enormous amount of time on that debate. The question should be how do you regulate in a way that is sufficient to produce good results and particular contexts? That does not allay -- does not lay on unnecessary burdens on operators and all those who have to ensure compliance, the regulatory organisations, but at the same time

the public interest needs to be protected. The idea of dynamic and responsive regulation. We talked about that with regard to spectrum but it can also apply to security. With security sometimes we try to come up with the perfect policy agreements before the fact. I'm not sure that is always possible. The Internet of Things, certainly, we need to look at the basic fundamentals that we need to, but not regulate every problem that might occur. I think one way of doing that is to develop principles. In telecoms we talked about -- I don't think that works necessarily in a more diverse context with different types of technologies and integration with online and offline factors, but I do think that principles, basic principles that respect human rights and that support public participation and transparency, principles of good governance as well as principles of social and economic inclusion. I think we tried that with the Mandela principles, that's a pretty good place to start.

Finally, we need good governance and I think we need that at multiple levels. That also, I want to come back to human rights, but I think the challenge in having a trusted and connected world is that you need to work both with consumer rights and fundamental human rights. These are two areas of rights that don't often work with one another, but in our context they are equally important. And capacity. Capacity at all levels remains important and includes capacity at the level of citizens and citizen organisations to hold others accountable, but also capacity at the level of the regulators and states.

>> KIM ANDREASSON: Thank you, Mrs. Esterhuysen. We are moving on to Mr. Van Tol, please?

>> WOUTER VAN TOL: Yes, thank you. So on this, I think Dr. Lee has set us a huge challenge here. Sets society a huge challenge. Let me just say which things and enabling factors I have seen work in my experience, because again that is where I need to start. People talk a lot about cooperation, but cooperation can be a built of a cliche. How do you do this? In our digital academies we are actually -- when I say we, I mean Samsung electronics. We have a Samsung lab inside

existing education institutions, whether that is professional training place or university. And being inside your partner's building is an entirely different type of cooperation than calling somebody from your office. It means that you are confronted with the real issues, with real people and you need to sort things out together. For me that is a very important enabling factor is close cooperation.

Second is that change can't just happen top-down. And it can't just happen bottom-up. It needs to be simultaneous. As it was just suggested by His Excellency, you know, government can pull together the right people, the right multistakeholders who might not otherwise speak to each other. That is an excellent way. And I support the idea about principles as well. The Internet of Things and cyber space more of so quickly and the threats change so quickly that you can't regulate it all. It can't be done. So an idea of principles is something that I would support.

But then the bottom-up approach is important as well. There's a lot of innovation going on literally on the -- well, in my case in classrooms around Europe. One thing I would specifically like to highlight is Samsung electronics in Italy a year ago started a campaign which has been repeated this year against cyberbullying. That is not necessarily something you might expect a company like a producer of devices to do. But this is a real issue for our target audience of young people. A target audience not commercially but target audience for our citizenship work. Therefore, we have put together a national plan of how to address the issue of cyberbullying, which is one of the very metive issues. That is very -- very Emotive issue. That is successful and we are rolling it out.

Next I want to mention the close cooperation and secondly the top-down and bottom-up cooperation.

>> KIM ANDREASSON: Thank you. I want to thank the panelists for such excellent remarks and for sticking to time which allows us to have a half hour of Q&A. I know there are remote

participants but I want to start taking a couple of questions from the room. Any questions for our panelists?

We have a question from the gentleman up here to my left. And please state your name, your organisation and also who the question is for, please. Thank you.

>> AUDIENCE: I am part of Iffat. I will speak in French. I am a member of Iffat. And I represent Switzerland at the Iffat General Assembly. The problem which we currently face is similar to another matter which I would like to mention briefly. If I asked you what are the five biggest sellers of weapons on the planet, you would come to the answer fairly quickly. Now, if I asked you what are the five permanent Members of the Security Council, which is entrusted with peace and security and which have a veto, you would come to the surprising conclusion that they are the same entities. All I can say is that this is something that shouldn't be repeated elsewhere.

So to try to go in slightly more multilateral direction, I think it is important for us to begin with the concept of digital responsibility. When users click "I accept" often they don't understand the 20 pages of legal text which appear before them. So their trust is somewhat limited. Digital responsibility is not just a matter for users. It is a matter for states, for businesses, for communities and others. And if we want another model to the one that we have now, we need to work on these issues of trust in a multilateral fashion, and if possible in a fairly rapid manner.

I remind you that in English you have two words: Trust on one hand and confidence on the other. In France there's only one word, (French word.) in German there's just one word) German word.) and the richness of the English language is that disparities and distinctions can be made between trust and concept. There's a difference between the two in English. We should be able to establish a discussion at three different levels: Citizens, communities, and businesses/states. Because balance has to be struck between them. We need to take into account when we are striking that balance of the

many different types of diversity which exist on the planet. UNESCO has published a booklet on diversity and mentioned 63 different types. It is not just gender or language or culture. It is something which is really very complex. I think we should delve deeply into this question and we should be quick about it, too. If we have a code of conduct in front of us, rather if we don't have one we could get into problems. If restrictions can be imposed on the Internet, we will see the fall out from that in the short-term. Has anyone thought about what would happen if three days went by where the Internet didn't work anywhere on the planet, for instance? We need to think about these things. If we're working in front of a computer screen, as I am here today. We are, we are part of a network. And we have to think about where the human responsibility lies when we are dealing with these machines. We really need to move towards this multistakeholder focus so that we can establish a certain number of principles. Transparency is crucial. And that's more important than security. I would even go so far to say that security is a byproduct of transparency. So I would urge all those on the panel here today and others who are participating in this conference to seize that bull by the horns and work concertedly, but in a multilateral fashion to be able to protect our future, which is something that we can tackle more enthusiastically than is sometimes the case.

Here in Geneva there is a restaurant with a tile on the wall that says tomorrow Beaujolais will be free. Here often the discussions which we have make me think of that. I've never had a glass of free wine in that restaurant because tomorrow never comes. I would like our enthusiasm to be fully implemented. I think we are all very positive, but I think it should become a concrete reality and we should be preparing for the future and embracing trust and confidence because they are just two ingredients. We will talk about the other ingredients tomorrow morning on the topic of IPV3 discussion. Thank you.

>> KIM ANDREASSON: Thank you for that intervention. Very much appreciated. I would like to turn it into a discussion

for His Excellency Ocampos. You all talked about trust but I will start with you. What are you doing in your country, Paraguay, to enhance trust?

>> DAVID OCAMPOS: Well, many of the measures which we've taken I've already mentioned to some extent, but we need to understand that we have embarked upon our digital Agenda now. That began two years ago in our government. And digital security is a cross-cutting element of that, as is infrastructure. Those are the two cross-cutting topics in our digital strategy.

The first thing we did is set up an IT incident response team. That's a preventive measure. Where cyber crime and cybersecurity are concerned, once the fault or the crime has been committed, it is very difficult to assuage the fallout from it. If a child has already been groomed, that's difficult to undo. And it is also very difficult to find the person that did it.

So these offices, these teams strive to prevent those offenses from being committed in the first place. We have security alerts and antidotes, so to speak, to prevent those offenses from being committed.

Campaigns, as I said before, are the most effective measure. We see peaks in offenses at certain times and they are often caused by what is going on in other countries. These crimes are often cross-border crimes. What is required to counter them is that we all act together. That's why it is good to set up these teams that I'm talking about.

Besides that, industry is a key consideration. Industry has been a very weak link in the chain. I'm talking about the training of technical experts and specialists in universities and technical colleges. They are often very professional in one sense but they are not so good at creating secure systems and robust networks. That's something we suffered from in Latin America. We need to work directly with industry so that the state-of-the-art where cybersecurity is concerned is implemented in full so that these people are aware of what's going on in the industry as long as they leave school or as

soon as they leave university. I would also like to go back to what was said in the first place. Without a national cybersecurity plan that comes from an executive decree, so from the legal framework of a particular country, it is very difficult to bring all the different stakeholders to the table. That should be the starting point because cybersecurity is a problem for all of us and for every sector. So we need laws, but we also need a round table where we can get everyone involved and discuss what is going on.

>> KIM ANDREASSON: Thank you very much, Your Excellency. Any other questions in the room?

We have a question in the back, in the middle. Please again, state your name and your organisation.

>> AUDIENCE: My name is (indiscernible) from Korea. I am working at the university. I listened to you and we established a trusting provision in our Forum. So we have started on that. So I want to show one important example. In France, this institute report is at first, in 2007 the trust in online was 17.1 percent. In 2013, trust in online rating was 51 percent, almost 20 percent increased. Another important report was from Boston. Economic economy increased, 25 percent recently. I think this is one of the problems is really the trust problems he mentioned like this. In this case, how do you think about this kind of situation for the future? Keeping the cyber space and online space on trusting the connected world? Thank you, Mr. Chairman.

>> KIM ANDREASSON: Thank you very much for the question. We are still on trust. I think all the panelists brought this up. I can probably hand it to any of them. Dr. Lee, why don't you give your additional perspective on the trust issue as the digital economy evolves.

>> CHAESUB LEE: Thank you very much, yes. I believe this is more in this nature because we have more and more cases of using the online environment, especially the Web environment. The provision is now available, but there is no credits about the contents. But we didn't talk about this quality of contents. This depends on each individual, their

responsibility. You can imagine some medical information you got from the website. Might be very dangerous, but there is no indications of the level of that content. I believe that this is why the cause of this decrease of this trust comparing it with the year 2007, the year 2013, something like that is my understanding. And we just add one more comment to the previous interventions from the floor. That this is one of my background why we think about technical community, the challenges on this. Many of you use laptops and smartphones, but you are not experts on all the details of the phones and laptops. Many of you are not experts on the IP technology, device technology, Web technology, we don't know. But we are good at enjoying, the use of these because there is a certain support from the technical community to use certain belief in these capabilities. So this is one of the reasons why I want to say this is a good time to take up the challenge on this. We are fastly moving forward with this cyber space. So it could be a good subject. We can challenge this aspect to protect this reduction in trust. The gentleman said there is one example. Within six years, 10 percent decrease. Then it could be next 2020, our trust might be less than 10 percent? That was not our goal, yes? That should not be our goal. This is the reason why we call this a connected trusted world.

>> KIM ANDREASSON: Thank you. Mrs. Esterhuysen, you wanted to add?

>> ANRIETTE ESTERHUYSEN: I wanted to respond to the speakers and Rick said earlier. We were involved in an initiative in South Korea where a group of lawyers and technicians and Civil Society organisations and businesses came together to develop a model law on security. And you know, that is an initiative that is a different approach. It is an approach of involving the stakeholders that are both responsible for providing security, some of them were Internet service providers, but also have a demand for security in developing a legal framework. I think this is what this more inclusive way of making policy and regulation allows us to do. That's a kind of innovation.

In response to multilateral and the speaker who talked about the need for more multilateral approaches here. I don't see the Security Council or the existing multilateral approach being all that successful in preventing wars or dealing with current conflicts. I'm not saying there isn't space for that, but I think that is a way of securing trust and security which also has limitations. I think being in this world we have different ways of doing it. I think we should utilize that.

I think just finally, something maybe that I didn't emphasize before, but I think the publicness is important, the publicness of the Internet. When we are talking about trust and a connected world, how do we understand this entity that we want to be trustable? And to facilitate more connection? I think that's something that we also lose sometimes in our conversation, in securing it for what and for whom? I think that is important as well.

>> KIM ANDREASSON: Great. Thank you, Mrs. Esterhuysen. Those are very good interventions because they add to the debate here. Mr. Van Tol, you wanted to add?

>> WOUTER VAN TOL: Yes. I just wanted to get a direct answer to the question from both gentlemen, especially the gentleman from Iffat. We already do some work in our 600-plus classrooms in Europe on child online safety. We also do some other things in our digital academies for the older group, 16 to 24 years old. What I'll take away from this and what I can promise the gentleman is that I'm going to after this session is over make a call to see if we can put cybersecurity into the curricula for those classrooms and digital academies.

Because I agree that we need to move faster than we are collectively.

>> KIM ANDREASSON: Thank you, Mr. Van Tol. Not to be left out, Mr. Samans, can we get your additional -- okay?

Any additional questions from the audience? Not at the moment? Do we have any remote participant questions?

I guess we don't have any remote participant questions but we have an in-room question. Please state your name and your organisation and.

>> AUDIENCE: Yes, I'm the Chair of the English chapter of the Internet Society. My question is as follows: The Internet is widely understood to be a reflection of the real world and yet there is no trust in the real world as such. Why are we trying to make the Internet more trustworthy than the real world is?

>> KIM ANDREASSON: That was a very good question. Who would like to ...

>> ANRIETTE ESTERHUYSEN: Maybe the other panelists want to respond as well.

Olivier, I agree with you. Particularly looking at child safety, for example, more children are abused in their homes and families than they are on the Internet. That is still the reality if you look at the statistics.

I think it is an issue. I think that is, I think policymakers need to come to terms with that. Parents need to come to terms with that. We all need to come to terms with that. We live in a changing world and building resilience and capacity in users to deal with those changes in children and young people, is far more important and sustainable than trying to create an Internet which is secure and which is so restricted of bad activity that it also ends up restricting good activity.

>> KIM ANDREASSON: Terrific. We have a couple of add digs. Dr. Lee first?

>> CHAESUB LEE: Yes, in my view, in my observation, in the physical world we have a certain level of trust. As an example, if I leave my smartphone in this room, maybe I guess I will -- if I return to this room I will find this smartphone. But if I left my smartphone on the train station, maybe I don't think if I return to the railroad station, it's just a waste of my time because we have certain understanding

of the level of trust. We didn't clarify this, but we have a certain mechanisms to mutually understand this level of trust.

Look at this cyber space. You know, our level in the current information environment, we didn't have such kind of case. Only some things, one popular way is ratings. People rating, someone rating? Or someone commenting? That is only what you have now. So I believe even our approach, our challenge to make this cyber space trusted, is not the same as the physical level. If we can not reach this physical level relatively, it's a good stage. My observation is still far behind. We have many, many areas to change, to realize practically realize the practical world into the cyber space.

>> KIM ANDREASSON: Thank you, Dr. Lee. Mr. Van Tol, you wanted to add something?

>> WOUTER VAN TOL: Yes. I wanted to thank you for your question, which I enjoyed very much. Of course, the premise of the question is entirely false because there is trust in society, but you can't trust anyone just like that. So let me give you a quick example of how I see it.

I was talking to my wife the other day about whether we would let our young daughter walk to the school or not unsupervised for the first time. Now, you can't regulate for my daughter specifically to walk to her specific school and not to be in any sort of risk. We have a framework of laws so that if something awful was done to her, hopefully the culprit is caught and punished. That's what we can do.

What you can do is educate her to the best possible way in all kinds of strategies to get from A to B without coming to any harm, right? And then you trust her and you trust society to get to school savely and back again. It is not that different. I agree that the Internet is very much like people. We saw that recently when people taught this robot, the artificial intelligence robot all kinds of awful things.

The Internet is pretty much like people. You need some regulation. You need some principles. You need some education. When all those things come together that is how it

will work. There will still be issues, but it's better than what it is currently probably.

>> KIM ANDREASSON: Thank you very much, Mr. Van Tol. Any other questions from the audience? We have a couple minutes left.

We have a question from the gentleman in the middle over here who raises his hand. Please state your name and the organisation you represent. Thank you.

>> AUDIENCE: I am speaking rugs. There is a lot of trust in the Internet because from the technical side of the Internet, it was built and it is still working because there is a great trust between operators building between other entities.

Also there are technological, technological ways to build and improve trust. When you are outside, you have a framework supporting your trust with your bank, but you are talking about different ways of trust. Now you are talking about technological ways, giving technical ways as an example of trust. Why is there no engineer supporting trust on this panel? Thank you.

Kim kitchen thank you very much for that question. I appreciate it.

>> KIM ANDREASSON: Thank you very much for your question. I appreciate it.

Dr. Lee, you are the head of technology for ITU. Maybe you can answer the question, please.

>> CHAESUB LEE: Yes, thank you for this question. I shared some views with this. Let me say too, simply two aspects. The first one is unfortunately we didn't use this trust language in technical terms. The use of trust in very normal terms, something high level, philosophical terminology. We didn't use this terminology in the engineering aspect. So this is my understanding.

So for example, we have quality of service. We have something, some security measures, security technologies, security mechanisms. But we don't have anything about trust.

Why we call this trust? We assume that someone trust, trust technologies, someone trusts the Internet. We believe this is a certain trust. But how we can measure this trust? This is a subject for measuring? Or this is a subject dealing with other capabilities? We didn't have that yet. This is my first observation.

Second one is in my Bureau, ITU, we have technical standards. We have certain discussions, several workshops that we had how we can bring all this trust into an engineering aspect. Some of the discussions are ongoing, trying to engineer a study to analyze the engineering aspect to implement the support of this trust. So we are going on. One of our study groups and also a technical report, trust is probably for future ICT services. That is, we will continue this study. It is in the very initial stage. It would be good to have a collection of our engineers, could be a good framework for multilevel development.

>> KIM ANDREASSON: Terrific. Mrs. Esterhuysen?

>> ANRIETTE ESTERHUYSEN: Very quickly. It is a good question. If you look at what is happening at the IETF and the research group, they are working on this. The engineers are absolutely vital. We also might be doing a little bit of reverse engineering. What happened is that business models developed on the Internet which were enormously innovative and productive, but these business models were based on lack of security. So to speak. On the ability of Internet companies to access their data, users behavior, metadata. And these business models became the business model on the Internet. Then the weakness and the insecurity of those business models became known to the world through Snowden and other revelations. Now we are trying to insert more trust and security into that.

There are limitations. As long as the business model is maintained, there is a fundamental insecurity in there. I do think the technical community is taking this on. I think the engineers are the ones that are going to help us with end-to-end encryption and just having a more secure Internet. I

think the possibility is there. They just need to be supported and given the opportunity. And we also need to look at business models that contradict some of those measures at a fundamental level.

>> KIM ANDREASSON: Excellent. We are coming up on time here, but I noticed that His Excellency Ocampos wanted to add to this as well. His Excellency Ocampos, you get the last word in this session.

>> DAVID OCAMPOS: I merely wish to add two things.

We are speaking almost on two levels in this panel. When we talk about security, when I am talking about myself, I'm talking about security for myself and the networks and teams. There is another level which is trust or confidence. This isn't done by networks and so on. It is people who put a stamp on these networks who provide this confidence. And yes, the Internet can be a more trustworthy world than the real world because when, for example, you buy something and the seller has a trust seal or a rating, it is something which is not done by my friends. It is something done by millions of people.

But when it depends on the prism through which we view the world we want to do some things, we can compare it to being in a train station and some other situations on the situation. Like leaving a phone in this room.

>> KIM ANDREASSON: Thank you, Your Excellency. That is the end of our panel because we are out of time. It was an excellent panel, if I had to pick up three things, trust came up from every panelist, the second was multistakeholder engagement, a great way to create trust and third, capacity building is across-cutting issue as well.

With that, the panelists, join me in thanking our panelists, Mr. Van Tol, His Excellency Ocampos, Ms. Esterhuysen, Dr. Lee. Thank you.

(Applause.)

(The session concluded at 1635 CET.)

***

This text is being provided in a rough draft format. Communication Access Realtime Translation (CART) is provided in order to facilitate communication accessibility and may not be a totally verbatim record of the proceedings.

***