

HLD4: Building Confidence and Security in Cyberspace

Thursday, 19 May, 09:00–11:15, (Governing Body Room) (E/F)



HLD No. 4 provided an interesting blend of an expert panel and audience interaction on Confidence and Security in Cyberspace

By bringing together governments, private sector, international organizations, civil society, and academia from all over the world, the High-Level Dialogue offered an opportunity to discuss in an interactive session the measures that can be adopted to foster an enabling environment to confidently use Information and Communication Technologies (ICTs). The growing incidence of cyberthreats and cybercrime, from financial and identity related frauds to illicit use of ICT services and applications, undermines the willingness to fully exploit the potential benefit of the Information Society, limiting the opportunity to use ICTs as enabler to improve effectiveness and efficiency of the online presence. Through the discussion, high-level panellists introduced challenges and solutions to build a safer interconnected world as well as best practices and actions that make difference in the cyberspace. Moderator:

Speakers

- Dr Hamadoun Touré, Secretary-General, ITU
- H.E. Mr Haruna Iddrisu, Minister of Communications, Ghana
- H.E. Mr Mohamed Nasser Al Ghanim, Director General – Telecommunications Regulatory Authority, UAE
- H.E. Mr Ilya Massukh, Deputy Minister, Ministry of Telecom and Mass Communications, Russian Federation
- Mr Mohd Noor Amin, Chairman, International Multilateral Partnership Against Cyberthreats (IMPACT)
- Mr John Mroz, CEO, East West Institute (EWI)
- Mr Rainer Wieland, Vice President, European Parliament
- Ms Marielos Hernandez, Executive President of PANI, Costa Rica (tbc)

Moderator: Dr Tim Unwin, Royal Holloway, University of London

Within the overall framework of the Global Cybersecurity Agenda (GCA), ITU has been entrusted to take a leading role in achieving cybersecurity and reinforcing international cooperation to address cyberthreat challenges globally. In this direction, the ITU–IMPACT coalition has been indicated as one of the key solutions of international cooperation and one of the best players to share best practices and international . As one of the major cyberthreats, child online protection-related issues were also discussed; ensuring safe and protected access to ICTs by children and youth requires international organizations to allocate technical and economic resources to carry out investigations using a human-rights-based approach. By building awareness and straightening national capabilities, the international community will be better prepared to face cyberthreats and fight cybercrimes.

The session ended with a call to strengthen international cooperation and coordination among agencies at national, regional and international levels.

Moderator: Dr Tim Unwin, Royal Holloway, University of London

Panellists:

Dr Hamadoun Touré, Secretary-General, ITU, stated that cybersecurity is one of the most important challenges in ICTs faced by the international community, and also one of the biggest tests in international cooperation. He informed that the ITU Global Cybersecurity Agenda (GCA) is built upon five strategic pillars 1) Legal Measures 2) Technical & Procedural Measures 3) Organizational Structures 4) Capacity Building 5) International Cooperation. He stated that cybersecurity is not an issue for only one country, but a global issue, and we are as strong as our weakest link. He also went on to state that the concept of a superpower is becoming obsolete, since in an increasingly technological world, every individual has the opportunity to become a superpower. For example, the Filipino author of the ILOVEYOU Bug wrote this devastating virus on a computer worth less than USD1000. In closing, Dr Touré emphasized the importance of protecting children as a normalizing, common denominator between all stakeholders.

H.E. Mr Haruna Iddrisu, Minister of Communications, Ghana, urged that improved legislation, which goes beyond data protection, needs to be put in place to more effectively deal with matters in cyberspace. He also highlighted that much of ICT infrastructure is owned by the private sector, and called attention to their role in the larger cybersecurity discourse.

H.E. Mr Mohamed Nasser Al Ghanim, Director-General, Telecommunications Regulatory Authority, UAE, emphasized the need for a legal framework for cybersecurity. He pointed out that although a number of countries have begun the creation and implementation of legal frameworks, agendas and roadmaps, many countries have not. This is a concern due to the transnational, borderless nature of cybersecurity threats, and international collaboration is the only way to effectively counter cybercrime.

H.E. Mr Ilya Massukh, Deputy Minister, Ministry of Telecom and Mass Communications, Russian Federation, pointed out that ICTs are a locomotive for local economy and increase in GDP, yet they are also a very attractive vehicle for unlawful and illegal elements. He stated it was of upmost important to discuss cyberthreats and encouraged multilateral cooperation. In closing he said that Russia is only one country and that one country cannot develop rules to govern the global phenomenon which is the Internet. To this end he reemphasized the role of international cooperation.

Mr Mohd Noor Amin, Chairman, International Multilateral Partnership Against Cyber Threats (IMPACT), drew parallels between infectious diseases and cybersecurity. He pointed out that during a disease outbreak there is international cooperation and coordination in moderating ports of entry. This model is possible through concerted global action and institutional assistance. The Chairman hoped to replicate this model for cyberthreats, using IMPACT as a vehicle.

Mr John Mroz, CEO, EastWest Institute (EWI), said that due to the increasing digitalization of the global economy, cyber criminality has been growing. He drew attention to the speed of advancements in technology in contrast to the slow adaptation and creation of agreements, policies, standards and regulations in which to govern them. He addressed the lack of trust between international actors and gave examples of some activities which encouraged discussion and built trust between countries: the Chinese-American partnership which aimed to tackle spam, and the Russo-American initiative to agree on 23 definitions. In closing he emphasized that more initiatives which provide solutions and build trust are needed.

Mr Rainer Wieland, Vice-President, European Parliament, addressed the speed at which technological advancement is increasing, which in turn creates new opportunities for cybercrime. The Vice-President urged the creation of a culture to combat cybercrime which is needed if we wish to build trust and confidence in our efforts. In closing he stated we must address and educate two parts of society: the younger generation who know more than their grown-up counterparts and the older generation who know far too little.

Ms Marielos Hernandez, Executive President of PANI, Costa Rica, reported on Costa Rica's efforts in adopting global online child protection. It included initiatives for training in prevention, educating children about cyberthreats, establishing guidelines for industry codes of conduct, and establishing national informational hotlines. The President, by presidential decree, also created the National Online Security Commission which is a multistakeholder and interdisciplinary initiative to deal with cyberthreats.

Questions	Responses/ Comments
<p>Dr Tim Unwin: What do you think is most important in building confidence amongst citizens with regards to cybersecurity?</p>	<p>Dr Hamadoun Touré, Secretary-General, ITU: re-emphasized that cybersecurity will only be achieved when we have a global framework and that the protection of children can act as a common denominator on which to build our efforts.</p> <p>Mr Rainer Wieland Vice-President, European Parliament: Ssaid that not everything considered by the government to be urgent is urgent to citizens. He posed the question “Do we have a legal agenda? And if so do we have a list of core crimes which can be commonly agreed upon?”</p> <p>H.E. Mr Ilya Massukh Deputy Minister, Ministry of Telecom and Mass Communications, Russian – Federation: Sstated that there is no single bullet for global cybersecurity regulations but that each country should take steps to protect citizens. He also emphasized the need for education, especially as it related to new trends such as digital signatures.</p> <p>Ms Marielos Hernandez Executive President of PANI, Costa Rica: Sstated that when we talk about children we have to talk about children within both a national and multidisciplinary, inter-institutional global framework. She also highlighted the need to teach prevention to parents and educators.</p>

Questions	Responses/ Comments
<p>Dr Tim Unwin: What is the biggest threat your country faces in terms of cybersecurity?</p> <p>Question from the floor: What are governments doing to encourage vendors to provide better support and produce less complex products which are more accessible?</p> <p>Comment from the floor: It is important to incorporate children into looking for solutions because they are better, and cyber criminals are also younger.</p>	<p>Mr John Mroz, CEO, EastWest Institute (EWI): agreed that the discussion of child protection creates awareness and that awareness is critical in making the dialogue on cybersecurity relevant to the general population. He pointed out that by age four children know to put on their seatbelt when in a car, but are unaware of basic cybersecurity principles and that this must be remedied through education.</p> <p>H.E. Mr Mohamed Nasser Al Ghanim Director-General, Telecommunications Regulatory Authority, UAE: pointed out that, due to the large amount of specializations, capacity building becomes extremely difficult. He stated that there is a need to train people on evolving threats on a monthly basis, and also that there is a need for basic awareness in actions such as not opening spam. At the end of the day it is about educating people's behaviours, not about technology.</p> <p>H.E. Mr Haruna Iddrisu, Minister of Communications, Ghana: raised the question of how governments can commit to the safety and security of cyberspace if cybersecurity is a transnational problem. He also raised Ghana's issue of younger people using IT for Sakawa, internet fraud, instead of productive capacities.</p> <p>Mr Mohd Noor Amin , Chairman, International Multilateral Partnership Against Cyber Threats (IMPACT) – highlighted the strong motivations and ideologies of cybercrime perpetrators and that only international collaboration can effectively counter them. He also raised the issue of the private sector in not sharing information regarding which systems have been compromised, and that they have a responsibility to share this information with the rest of the world – which, up to this point, has not been done.</p> <p>Dr Hamadoun Touré, Secretary-General, ITU: stated that emphasis should be placed on what we hold in common (protecting our children) in order to develop a competent framework which can be extended to other areas.</p> <p>H.E. Mr Ilya Massukh Deputy Minister, Ministry of Telecom and Mass Communications, Russian-Federation: used the example of child pornography to build an international framework of regulations.</p>

Questions	Responses/ Comments
<p>Comment from the floor: Cybercrime is not a technical issue; it is an economic, societal issue. It is important to understand the fundamentals and what you trying to protect against. It is important to define threats properly.</p> <p>Comment from the floor: The definition of cybersecurity not as important as solutions. Cyberspace needs to be conceptualized differently. It has economic, technological and environmental dimensions. A comprehensive cyberspace law would be an endless exercise. One approach to think about could be one approach for each dimension, rather than trying to find a full comprehensive law which covers all those aspects and touches all those elements.</p> <p>Dr Tim Unwin: Will policies always being playing catch-up to technological change? Or is there something we can do?</p> <p>Dr. Tim Unwin: How should the international community better commit to the online protection of children?</p> <p>Remote Participant: What can we do to raise awareness about cybersecurity outside of the Internet?</p> <p>Comment from the floor: This person wanted to emphasize the need to educate people in conceptualizing ICTs in terms of how they can be used productively and maliciously.</p> <p>Comment from the floor: This person wanted to point out the need for training of law enforcement to understand the new paradigms in cybercrime definitions, such as the theft of personal data.</p>	<p>Mr John Mroz, CEO, EastWest Institute (EWI): emphasized the special nature of cyberspace regarding the application of the Hague and Geneva Conventions. He stated that a new way of thinking is required to effectively deal with cybersecurity and that we need to involve ourselves in discussions surrounding cybersecurity issues.</p> <p>Mr Mohd Noor Amin, Chairman, International Multilateral Partnership Against Cyber Threats (IMPACT): talked about IMPACT's initiatives for capacity building, including workshops, and stated IMPACT's willingness to respond to cyberthreats.</p> <p>Mr Rainer Wieland, Vice-President, European Parliament: stated the need for a clear definition of cybercrimes and the need to find a code of conduct for international procedures in prosecution.</p> <p>Dr Hamadoun Touré Secretary-General, ITU: stated that the nature of technology will always put it ahead of legislation, and that we need to operate as though we are in a time of war, with a strong code of conduct and best practices for Member States to follow. He re-emphasized the need for action and not deliberation.</p> <p>Mr John Mroz stated the need for better measurement tools of cybercrime, and also the need for the private sector to cooperate in reporting how cybersecurity is affecting them.</p> <p>H.E. Mr Haruna Iddrisu, Minister of Communications, Ghana: stated his wish would be for more international cooperation.</p> <p>H.E. Mr Mohamed Nasser Al Ghanim also stated the need for further cooperation with emphasis on urgency and commitment.</p> <p>Mr Mohd Noor Amin wished to see the acceleration of the establishment of a cybersecurity framework. He also stressed the need for true international cooperation.</p> <p>Ms Marielos Hernandez stated that we need to take a human rights approach by investing in education and health. She also stated that we need to listen to and include children in the discourse of tackling cybersecurity.</p> <p>Dr Hamadoun Touré asked how we can avoid ideological fights within cybersecurity discourse and restated the need for focusing on our common factors, namely children.</p>

Questions	Responses/ Comments
	<p>H.E. Mr Ilya Massukh also re-emphasized the need for focusing on the common denominator, child pornography, as a foundation for producing an international framework. He also highlighted the need to regulate social networks more strictly due to the high amount of child participation.</p> <p>Mr John Mroz applauded the awareness raising and highlighted the vast set of problems that the global community has to deal with. He closed by emphasizing the need for action-based initiatives.</p> <p>Mr Mohd Noor Amin re-emphasized IMPACT's agenda for capacity-building and an invitation to utilize the training and programmes offered by IMPACT.</p> <p>Mr Rainer Wieland shared his surprise that nobody brought up state criminality in the cybersecurity discourse. He stated that we need to address it at the UN level and resolutions are needed to effectively engage it.</p> <p>Dr Hamadoun Touré highlighted ITU's role in awareness-building, not only through the Member States but also through the partnership with 700 private companies. He went on to state that a new global treaty would be needed for cyberspace – no longer will it be restricted to countries but it should also involve corporations and the private sector.</p> <p>H.E. Mr Haruna Iddrisu called for the need of a comprehensive framework that was still mindful of differences between countries and cultures.</p> <p>H.E. Mr Mohamed Nasser Al Ghanim said prerequisites will be needed for a global treaty, proper response rates and the need for international actors to take violations seriously. He also stated the need for the private sector to participate in a larger global framework due to their deep involvement in ICTs.</p> <p>H.E. Mr Ilya Massukh agreed that the private sector should be involved in the discussion of a global framework. He also stated that the dialogue for cybersecurity has been started at the right time and restated the need for fighting child pornography.</p> <p>Ms Marielos Hernandez stated the importance of allowing children and younger people to participate in the larger discussion of cybersecurity. She also re-emphasized the need for articulation in agreements.</p>

Please note that this summary only provides a snapshot of the high- level dialogue. The complete Webcast of this high-level dialogue is available at:

<http://www.itu.int/ibs/WSIS/201105forum/index.html>