ITU Workshop on ICT Security Standardization Challenges for Developing Countries

15 September 2014

ITU Headquarters, Geneva

Opening Address

Malcolm Johnson

Director, Telecommunication Standardization Bureau  
International Telecommunication Union

Friends and colleagues

Ladies and gentlemen,

Good afternoon and welcome to this workshop on “ICT security standardization challenges for developing countries”. Greetings from Secretary-General Hamadoun Touré who unfortunately was unable to be with us for the opening today. I am pleased to say Director Brahima Sanou hopes to join us for the closing tomorrow.

The World Summit of Information Society gave ITU a mandate to build confidence and security in the use of information and communication technologies (ICTs).

This is an extremely challenging task. And I would like to take this opportunity to thank the experts of ITU-T Study Group 17 for the dedication to the group’s complex objectives. In particular, I must thank the Russian Federation for its enduring support to SG17 in the leadership that Mr. Arkadiy Kremer has provided the group over the past six years. The SG17 meeting starting on Wednesday once again sees an increase in participation – 33% increase on the previous meeting including 15 members attending for the first time, and a 30% increase in contributions compared to the previous meeting, as well as many proposals for new work. I hope this workshop will encourage even more participation. My TSB colleagues will be happy to answer any questions that you may have on how to become more involved in our work.

The workshop will discuss the challenge of cyber threats – a common threat to the world but especially in developing countries which, now have an equal and growing share of the origins and destinations of cyber attacks as developed countries.

As ICTs become prevalent in all walks of life these attacks are becoming more ever more critical both to society and businesses. Their increasing sophistication makes us ever more vulnerable to attack.

Spam is a particular concern to developing countries, undermining these countries’ efforts to ensure an adequate quality of service as networks expand to meet rising demands for data.

The World Conference on International Telecommunications (WCIT-12) in Dubai agreed the inclusion of a new article on the International Telecommunication Regulations (ITRs) encouraging Member States to cooperate to prevent unsolicited bulk electronic communications – the term used in ITU-T to refer to spam.

The ITRs gives strong impetus to the work of ITU-T as it underlines the value of adherence to international standards.

Standardization is an essential tool in our defensive against attack. This workshop and others like it are crucial in building an understanding of ITU-T’s security standards and how to apply them effectively.

National laws are often inadequate protection, unable to keep pace with the constant evolution of cyber threats and are frequently nullified by the trans-national nature of attacks.

In addition, a globally recognized legal framework to address cybercrime has been very difficult to achieve, with the Council of Europe’s Budapest Convention on Cybersecurity having been ratified by less than a quarter of the world’s countries since it was adopted in 2001.

This means that our defenses must be largely technical, procedural, and administrative measures that are internationally applicable. International standards are tools offering exactly this form of defense.

Standards bodies such as ITU-T therefore have a very significant role to play in encouraging international cooperation on issues related to ICT security.

ITU is not alone in this endeavour. ITU-T has developed collaborative relationships with a range of other standards bodies active in the security arena to deliver coordinated and complementary standards for today’s converged networks.

We also complement our technical work on ICT security with efforts to stimulate international cooperation in the development of security capabilities.

ITU assists countries in their establishment of mechanisms such as Computer Incident Response Teams (CIRTs). These mechanisms employ technical tools such CYBEX, the ITU-T X.1500 series of Recommendations, which allows the structured exchange of cybersecurity information.

These technical tools must be integrated with corporate and national security policies – all under the umbrella of a global cooperation framework.

Since its inception, the International Multilateral Partnership Against Cyber Threats (IMPACT), has worked closely with ITU, and is now the ITU’s executing arm for cybersecurity.

The ITU-IMPACT initiative comprises some 149 countries that have decided at the highest level to cooperate together. This is a unique alliance in today’s world, bringing together so many countries as well as industry experts.

And finally, ITU’s Child Online Protection initiative is promoting the development of a safe and secure cyber world for future generations – in conjunction with partners from civil society, international organizations and the private sector.

We are fortunate to have so many leading experts in the field as speakers and moderators in this workshop, spanning the public and private sector as well as developing and developed countries, and including many of our partners in this work. I would like to thanks them all for their willingness to contribute to this event.

I encourage you all to enter into an open discussion, and hope that we can conclude tomorrow with some suggestions for action that we can take forward that will help developing countries be better prepared to tackle the critical issue of security.

Thank you. I wish you all a most productive and enjoyable workshop.