ITU-UNODC
Asia-Pacific Regional Workshop
on
Fighting Cybercrime
21 September 2011
Seoul, Republic of Korea

Welcome Remarks
Eun-Ju Kim Ph.D.
Regional Director
ITU Regional Office for Asia and the Pacific

Excellency, Mr. Han, Prosecutor-General of the Republic of Korea,
Dr. Kim, President of the KIC,
Mr. Suh, President of the KISA,
My colleague, Mr. Lewis, Regional Representative of the UNODC,
Distinguished participants,
Ladies and gentlemen.

On behalf of ITU, first of all, I would like to welcome you all the participants to the Asia-Pacific Regional Workshop on Fighting Cybercrime. We would like to express our gratitude to the Supreme Prosecutors Office of the Republic of Korea, for the kind hosting this joint UNODC-ITU Workshop with support from the Korea Institute of Criminology (KIC) and the Korea Internet Security Agency (KISA).

It gives me great pleasure to be here today with our UN family member, the United Nations Office on Drugs and Crime (UNODC), as we together could bring in the common pool of experts and participants from both legal and technical community. I am sure everyone in this room recognizes how critical this cooperation is as criminals add devices such as computers and handheld ICT tools to their armory.

In recent times, we have seen so many attacks on organizations and countries so that the concern is no longer security of networks but a matter of national security. The need is not just for policy makers and law enforcers but also for law makers.

According to the 4th Parliamentary Forum on Shaping the Information Society, held from 18 to 20 May 2011 in Geneva, Switzerland, where the declaration recognized the importance,

> "*Confidence in cyberspace is vital for the development of the information society. As parliamentarians, we have the responsibility to enact legislation that promotes a safe and enabling environment for citizens, businesses and institutions to fully benefit from the Internet revolution, without constituting a threat to the peace and sovereignty of societies and in accordance with the principles of the World Summit on the Information Society.*
>
> *Yet, the Internet knows no borders. We recognize that cybercrime and the illicit use of ICT cannot be combated effectively without greater harmonization of our national legislation. The lack of harmonization creates an environment, in which criminal activities can proliferate in relative impunity, and it is therefore urgent to act promptly.*"

A fundamental role of ITU, following the World Summit on the Information Society (WSIS) and the ITU Plenipotentiary Conference 2010, is to build confidence and security in the use of Information and Communication Technologies (ICTs). At the WSIS, Heads of States and world leaders entrusted the ITU to take the lead in coordinating international efforts in the field of cybersecurity, as the sole Facilitator of Action Line C5, "Building confidence and security in the use of ICTs".

In response, ITU Secretary-General, Dr. Hamadoun Touré launched the Global Cybersecurity Agenda (GCA), which is a framework for international cooperation aimed at enhancing confidence and security in the information society.

This has been reinforced time and again at various highest level decision making meetings of the ITU such as the Plenipotentiary Conference (Mexico 2010), World telecommunication Development Conference (India 2010) and World Telecommunication Standardization Assembly (South Africa 2008).

However, tasks such as these cannot be done alone as well as require for engagement and cooperative frameworks amongst and within countries. The ITU in its Global Cybersecurity Agenda has recognized five main areas including: e.g. Legal Measures; 2. Technical and Procedural Measures; 3. Organizational Structure; 4. Capacity Building; and 5. International Cooperation, about which my colleagues will provide you with more details in their presentations over the coming three days.

The work ranges from developing appropriate standards, providing technical assistance, building human capacity and promoting international cooperation with relevant organizations. Along these frameworks, we have also instituted partnerships with organizations to work together in a number of areas. Today, this joint workshop is an example of our Memorandum of Understanding with UNODC to work together. Indeed, it is the first time that two UN bodies have formally agreed to work together globally on Cybersecurity and cybercrime, and you will hear on the existing and planned activities.

We also have with us International Multilateral Partnership Against Cyber Threats (IMPACT), which is the executing agent of ITU on Cybersecurity, where the ITU Global Cybersecurity Agenda is hosted. ITU and IMPACT now are one of the bigger - if not, the biggest - coalition on Cybersecurity in the world with 136 Member States formally accepted to be part of it. In keeping with the public-private partnership (PPP) tradition, ITU has also signed an MoU with Symantec, under which Symantec will avail quarterly Internet Security Threat Reports to increase awareness of and readiness for Cybersecurity risks among the ITU Membership.

In the Asia-Pacific Region, ITU, together with IMPACT and in partnership with ASEAN, is currently undertaking individual country CIRT assessments in Cambodia, Lao PDR, Myanmar and Vietnam (CLMV) to review the capacity and readiness of their respective national CIRTs in identifying, responding and managing cyber threats, in order to provide practical and actionable recommendations and eventually to enhance the Cybersecurity posture of the these countries and sub-region. Related to this, a CLMV Cybersecurity Workshop will be organized in November 2011 in Yangon, Myanmar. We have also carried out CIRT assessments in Afghanistan, Bangladesh, Bhutan, Maldives and Nepal, while assisting several countries with related policies. A dedicated centre for building capacity on these issues within the ITU Asia-Pacific Centres of Excellence has been also instituted in partnership with the IMPACT.

Dear friends,

In this era of broadband or converged ICTs, ensuring Cybersecurity and fighting against Cybercrime is not a choice but a must to ensure cyber peace. I think you will agree that Republic of Korea, which has ranked as the number one in the world demonstrating its leadership in the ICT Development Index (IDI) as per the *ITU's Measuring the Information Society 2011 Report* launched last week, is a great or right place to talk about it. I am sure that we will hear from the experts on how these issues are being handled here. I am also thankful to our experts, who have traveled from Europe and the Asia-Pacific, to share the wide international experiences on this critical matter.

One of the critical success factors to fight against Cybercrime is to have effective implementation and to set up national and international communication platforms, which can quickly and appropriately respond to the threat. I am sure that during the workshop, we will be able to identify what we can do at national, regional and international levels to strengthen the ongoing initiatives.

While looking forward to every success of this seminar, last but not the least,

I wish you to enjoy not only the seminar but also the rich culture of Republic of Korea, especially at the green or environment-friendly city of Seoul.

Thank you very much for your kind attention.