International Telecommunication Union

Australian Government
Department of Broadband, Communications and the Digital Economy

Opening Remarks 16 July 2008

ITU Regional Cybersecurity Forum for Asia-Pacific[1]

Brisbane, Australia
16-18 July 2008

Eun-Ju Kim
Head, ITU Regional Office for Asia-Pacific

Honourable Mr. Keith Besgrove, First Assistant Secretary, Department of Broadband, Communications and the Digital Economy (DBCDE), Australia

Mr. Sahib Dayal Saxena

Mr. Joong Yeon Hwang, President and CEO of Korea Information Security Agency (KISA)

Distinguished Guests, Delegates, Speakers,

Dear Colleagues,

Ladies and Gentlemen,

Good morning. It is my great pleasure and honour to welcome you, on behalf of the International Telecommunication Union and the Director of the ITU Telecommunication Development Bureau, Mr. Sami Al Basheer Al Morshid, to this ITU Regional Cybersecurity Forum for Asia-Pacific where I hope that all of you will have discussions of a most rewarding nature. I am honoured to be

[1] See the ITU Regional Cybersecurity Forum for Asia-Pacific website at www.itu.int/ITU-D/cyb/events/2008/brisbane/

present here at the opening of this important event. I am particularly pleased to be amongst all the country delegates with us here today, as it confirms the importance and commitment given to this topic by countries in the region, whilst welcoming delegates from other regions too like the Americas and the Arab States.

I am also very happy to see so many distinguished speakers from the region as well as experts who have travelled from afar to share their experiences with us during this meeting. The list of speakers and participants is very impressive and I am sure this event will be beneficial to everyone and contribute to a deeper understanding of this very interesting and critical subject in the Pacific as well as the rest of the world.

Cyber-threats have become increasingly sophisticated since the early 1980s, when the first known case of a computer virus was reported. Today, cybercrime has become an organized and underground economy reaping vast financial rewards as we learned yesterday using sophisticated software tools, which threaten users and information infrastructures in all countries. Sometimes the biggest threats are simple accidents. This was demonstrated only a few months ago when millions of users in the Middle East were impacted by cuts in undersea optical cables – said to be caused by an adrift boat anchor.

In fact, it also happened here in the Queensland, Australia, yesterday morning, when I tried to submit documents online before the deadline. In these cases access to the Internet, voice calls, corporate data and video traffic were all impacted. Thus, I learned that the Australian government and industry requested backup after the optical cable cut. Just a few weeks ago, moreover, we saw one of the countries in this region, more specifically the Marshall Islands, experiences disruptions that paralyzed e-mail communications in the country. Reports say that hackers had launched a "zombie" computer attack on

the western Pacific nation's only ISP. It has been said that experience is the hardest teacher, because it gives the test first and the lesson afterwards. Whatever the cause, whether intentional or not, and whether a cybercrime or a mundane accident, the lesson we take away from these incidents is that every nation needs to prepare and organize itself to take comprehensive and coordinated actions related to the prevention of, preparation for, response to, and recovery from cyber incidents – i.e., a chain of actions for the whole spectrum of cybesecurity, we raised yesterday by delegates.

Yesterday, as many of you know, we started off with a one day Seminar on the Economics of Cybersecurity, chaired by the Chairperson of ITU's Tariff Group for Asia and Oceania (TAS), Mr. Saxena. We learned about the financial aspects of network security and the new revenue streams that are created from malware and spam. How they enable legitimate business models (e.g., antivirus and anti-spam products, infrastructure, and bandwidth) as well as fraudulent and criminal ones (e.g., renting out of botnets, bullet proof hosting,commissions on spam-induced sales, pump and dump stock schemes). We heard from distinguished experts in this area that malware and spam create mixed and sometimes conflicting incentives for stakeholders, which complicate coherent responses to the problem.

This Regional Cybersecurity Forum is one of a series of regional cybersecurity events that the ITU Development Sector is holding in response to requests made by our membership during the World Telecommunication Development Conference (WTDC) in Doha in 2006. Australia has long been a leader in developing national capacity to fight cybercrime and combat spam. By agreeing to host this regional cybersecurity forum, Australia - its Department of Broadband, Communications and the Digital Economy (DBCDE) in particular - is further showing its commitments to support ITU and its ongoing cybersecurity-related efforts. On behalf of the ITU, I wish to relay our special thanks to His

Excellency, Senator Stephen Conroy, Minister for Broadband, Communications and the Digital Economy (DBCDE) of Australia for his personal presence later on today, in spite of his busy schedule, Honourable Mr. Keith Besgrove, and his team, especially Mr. Colin Oliver, Dr. Jason Ashurst, Dr. Sabina Fernando, Ms. Annaliese Williams other national agencies and regional collaborators who have worked closely with us to assure this event would be a success. We recognize that Australia and DBCDE have played an important national and regional leadership role in cybersecurity and we look forward to continue working closely with you in the future. I also want to thank the Pacific Island Telecommunications Association (PITA) to join us as a partner in this event. We are also delighted to welcome the CEO and President of the Korea Information Security Agency (KISA), Mr. Hwang, Joong-Yeon, to this meeting here in Brisbane.

Dear Colleagues,

The ITU is committed to ensuring that we meet the needs and requirements of our membership of 191 Member States and over 700 private sector members. In the ITU's Development Sector, this is done through our programmes and initiatives that were developed at the WTDC in Qatar in 2006 and approved at our Plenipotentiary conference in Turkey also in 2006. We are aware that the issues raised by our membership are real needs for close cooperation from both the public and private sector to ensure all the citizens of the world to improve access to information and communications technologies (ICTs) and improve their lives as well as economical and social status in a longer run.

Recognizing the importance of international cooperation for cybersecurity, leaders from around the globe at the World Summit on the Information Society (WSIS), held in two phases in 2003 and 2005, entrusted ITU to play a leading role in coordinating the worldwide response to these global challenges. This is

why, just over a year ago on 17 May 2007, ITU launched the Global Cybersecurity Agenda (GCA), which is the ITU framework for international cooperation aiming at proposing strategies for solutions to enhance confidence and security in the globalized information society. Through the establishment of a multi-stakeholder High Level Experts Group (HLEG), GCA builds on existing national, regional and international initiatives to avoid duplication of work and encourage collaboration amongst all relevant partners. The HLEG advises ITU's Secretary-General on global strategies in all five work areas of the GCA. In this regard, I am pleased to share with you some of the recent initiatives by ITU Secretary-General, such as:

1) Collaboration with the International Multilateral Partnership Against Cyber Terrorism (IMPACT) initiated by Malaysian Prime Minister, as one of the physical homes for the GCA;

2) A series of interviews and meetings with Japanese Prime Minister and numerous ministers during OECD Ministerial in Seoul as well as media during his recent missions to Japan and Korea with the objectives to combat cybercrime in addition to climate change and roles of ICTs; and

3) A special High Level Segment session on cybersecurity will be held at the forthcoming ITU Council in 2009, which the Malaysian Prime Minister together with other Heads of States have been invited to attend.

Should there be any organizations and countries interested in exploring possibilities of collaboration with the ITU to meet the GCA goals, we would be happy to pursue various ways of the public-private partnerships.

At dawn of the 21st century, as the modern or information societies became more depending on ICTs with interconnected global villages, so is ITU committed to connecting the world. Such global interconnectivity creates new kind of interdependencies and risks that need to be managed at national,

regional and international levels. The formulation and implementation by all nations of a national framework for cybersecurity and critical information infrastructure protection (CIIP) represent a significant first step in addressing the challenges arising from globally interconnected ICT infrastructures, services and applications.

In practice, our development activities on this issue have been implemented through multiple but interrelated pillars at national, regional and international levels. First, one of ITU-D Study Group is developing a Report on Best Practices for a National Approach to Cybersecurity. During this event, you will hear more about the detailed frameworks, which include:

1) Developing a national cybersecurity strategy;
2) Establishing national government-industry collaboration;
3) Creating a national incident management capability;
4) Deterring cybercrime; and,
5) Promoting a national culture of cybersecurity.

The second is our Cybersecurity Work Programme to Assist Developing Countries, which sets out a detailed description how we are working with ITU Member States and Sector Members to develop cybersecurity capacities. In this regard, a joint ITU-D and ITU-T Sectors' Regional Workshop on Frameworks for Cybersecurity and Critical Information Infrastructure Protection was held in Hanoi, Viet Nam, in August last year, and some of you might have participated at the workshop. Moreover, our regional and area offices in the Asia-Pacific region have been assisting and responding to the needs of various member countries through providing experts, organizing trainings or seminars, or even sending the appropriate equipments on this matter. More details on the various ITU global and Asia-Pacific regional activities and initiatives are available at the registration desk.

Taking this opportunity, I would also like to draw your special attention to the unique challenges and needs for the Pacific Island countries relating to cybercrimes, laws and legislation. Last year, the ITU with the support from the Government of Australia, APT and PITA carried out a workshop with the policy makers of these countries on the “Principles of Cyber Legislation”. The workshop discussed the status of cyber legislation and also arrived at certain principles and a possible roadmap. Most of all, recognizing the critical risks experienced by Cook Islands, Solomon Islands and others, ITU has been assisting the Pacific Island countries in their submission of the Number Hijacking Resolution to ITU’s World Telecommunication Standardization Assembly (WTSA) to be held in South Africa later October this year. Reflecting all these challenges and needs, we have also scheduled some special sessions for the Pacific Island countries here during this regional workshop, whilst looking forward to some concrete recommendations from the sessions in this very workshop so that you can share the outcomes with other fellows, policy makers and decision makers for the appropriate policy and directions from preventing to recoveries from the cyber incidents.

Dear Friends,

In short, cybersecurity is a broad and complex topic. The goals and tasks ahead of us are huge, whilst resources are limited. However, all of us at the ITU are committed to not only connecting the world but also combating the cybercrimes in the interconnected and secured information society. I do not want to take too much of your precious time, so I will conclude now.

But before I do so, I thank you all in advance for your contributions to this event as well as the Government of Australia – especially the Broadband,

Communications and the Digital Economy (DBCDE) - for the never-ending efforts and generous hospitality.

I wish you all a successful event and an enjoyable time at this great city of Brisbane.

Thank you for your kind participation and attention.