



Opening Remarks 23 September 2009

ITU Regional Cybersecurity Forum for Asia-Pacific - Connecting the World Responsibly -¹

Hyderabad, India
23-25 September 2009

by Sami Al-Basheer El Morshid
Director, Telecommunication Development Bureau (BDT), ITU

Your Excellency Thiru A. Raja, Minister of Communications and Information Technology
Honorable Thiru Siddhartha Behura, Chairman Telecom Commission
Thiru Kuldeep Goel, Managing Director, BSNL
Distinguished Delegates,
Guests,
Ladies and Gentlemen,
Dear Colleagues,

Good morning.

I am honoured to be here this morning to provide these opening remarks on behalf of the International Telecommunication Union and especially the ITU's Telecommunication Development Bureau for which I am the Director. This **ITU Regional Cybersecurity Forum for Asia Pacific** is dedicated to the theme of "Connecting the World Responsibly". At the World Summit on the Information Society (WSIS), held in two phases in Geneva 2003 and in Tunisia in 2005, leaders from around the globe recognized the important role of Information and Communication Technologies (ICT) in stimulating employment, economic growth and social development. They also developed and committed to the WSIS *Plan of Action* to improve access to ICT in all parts of the world. Efforts are now underway to accelerate progress in meeting the goals of the Summit. In the Asia Pacific region, a number of important regional events have taken place during the past few years to mobilize resources for implementation of many initiatives related to infrastructure development, applications and services.

¹ See the ITU Regional Cybersecurity Forum for Asia Pacific website at: www.itu.int/ITU-D/cyb/events/2009/hyderabad/

When countries are rolling out large scale projects — such as e-government, e-health and e-education services — and increasingly interacting with citizens over the internet, it is all the more important that networks and connections are robust, secure and reliable.

Cybersecurity issues are a complex mix of technological, political, and cultural challenges. With the number of mobile cellular subscribers having reached 4 billion and the global mobile penetration rate estimated at 61 per cent at the end of 2008, I hardly need to remind you what a key role that the ICT sector has come to play in our lives. Access to ICTs has now become essential for social and economic development and provides solutions to a wide range of everyday problems. Today's young generation takes for granted the role that ICTs play daily in their education and private lives, welcoming new technological advances that are appearing at an impressive rate.

In this regard, one of the best examples of this is what we can all witness in this great country, India, where the growth of ICTs has been remarkable.

However, as new technologies are developed and global access to ICTs expands, threats to ICT security are also developing and expanding. These threats are global in nature, with attacks in one country having an impact on another, while the individual generating the attack could be sitting physically in a third country. Therefore, to safeguard our collective cybersecurity we have to have a global approach and come to a common understanding on how we can address the needs of all countries, including least developed, developing and developed countries. **Only by working together to elaborate strategies and identify best practices, can we address these global challenges.**

During these three days here in Hyderabad we will have a number of expert speakers presenting on national, regional and international initiatives and partnerships, as well as tools and practical ways to move forward on building confidence and security in the use of ICTs to ensure that their benefits reach all people in all parts of the world. This event also serves as follow-up to the activities initiated at last year's **ITU Regional Cybersecurity Forum for Asia and the Pacific**, held in Brisbane, Australia in July 2008².

I want to emphasise that cybersecurity is increasingly important in this region, and governments need to be well informed and coordinated on this topic. We hope that the presentations and training provided during these three days, and more importantly, the discussions and sharing of experiences

² See the website for the ITU Regional Cybersecurity Forum for Asia-Pacific and Seminar on the Economics of Cybersecurity held in Brisbane, Australia (15-18 July 2009) at: www.itu.int/ITU-D/cyb/events/2008/lbristbane/

and best practices that take place, will provide a useful foundation on which to further discuss these important issues amongst different stakeholders in the region.

Of course, I would like to share with you a brief overview of some of the activities that the ITU, its different Sectors, and Regional and Area Offices around the world are working on to help ensure that all parties, countries and private sector participants, academia and civil society, work together on fighting cybercrime and improving cybersecurity for all.

To put the activities and initiatives that ITU is working on in the area of cybersecurity, cybercrime and child online protection into context, two years ago in May 2007, ITU launched the **Global Cybersecurity Agenda (GCA)**. Designed as a mechanism and framework for international cooperation and response, the GCA focuses on fostering synergies and building partnerships and collaboration between all relevant parties in the fight against cyber-threats within five main work areas. These five work areas are: 1. Legal Measures; 2. Technical and Procedural Measures; 3. Organizational Structures, 4. Capacity Building, and 5. International Cooperation.

Since the launch of the GCA, and as part of the efforts mentioned earlier, the ITU Telecommunication Development Sector has been working on implementing activities related to the GCA, developing practical tools and resources that can be of use to ITU Member States looking to build cybersecurity capacity.

We are very pleased with the progress on the collaboration between ITU and the International Multilateral Partnership Against Cyber Threats (IMPACT), aimed at making available to Member States concrete cybersecurity measures such as the Global Response Centre (GRC) and tools to help countries establish a national Computer Incident Response Team (CIRT). This allows countries to prepare themselves against cyber threats, and ensure at the same time coordination and cooperation at the national and international levels. More than 30 countries around the world have already joined this ITU-IMPACT initiative and I encourage those Administrations present at this forum to contact my ITU colleagues for further information. We have also colleagues from IMPACT with us here this week, who will be sharing with us more information on some of the services that are being made available to ITU's 191 Member States.

Some other key cybersecurity deliverables include a set of dedicated cybercrime legislation resources aimed at helping countries better understand the legal aspects of cybersecurity in order to combat cybercrime and facilitate international cooperation. This includes the recently launched **ITU publication "Understanding Cybercrime: A Guide for Developing Countries"**, which you will be hearing more about this week.

We are also working to assist countries in elaborating national cybersecurity strategies, and tools such as the **ITU National Cybersecurity/CIIP Self-Assessment Tool**, which has recently been revised and can be of help in evaluating the level of preparedness and identifying possible follow-up actions to move forward on developing national cybersecurity capacity.

Furthermore, together with other stakeholders and experts, including many of you here today, ITU is working on establishing close partnerships with regional and international organizations, private sector companies, associations, etc., in order to be able to provide ITU Member States with the support and assistance that countries are increasingly requesting from us.

With this I will conclude my opening remarks. I want to thank you all in advance for your participation and contributions to making this Regional Cybersecurity Forum happen here in India. I would also like to draw your attention to the **ITU World Telecommunication Development Conference** which will take place here in Hyderabad in May next year. We hope of course to see you here again in May 2010!

Finally, I want to express our thanks and appreciation the Indian Ministry of Communications and Information Technology for their generosity and kind hospitality, and the Government of Australia, the Department for Broadband, Communications and the Digital Economy (DBCDE), for their contribution to this forum and for all Member States and Sector Members of this region for their continuing support to our activities.

Thank you and my best wishes for a successful Forum.