



Regional Workshop on Frameworks for
Cybersecurity and Critical Information
Infrastructure Protection

28 August 2007
Original: English

**Meeting Opening Remarks on behalf of
ITU-D Director Mr. Sami Al Basheer and
ITU-T Director Mr. Malcolm Johnson**

H.E. Mr. Vu Duc Dam, Vice Minister of Information and Communications of Vietnam,

Distinguished Speakers, Guests and Delegates,

Ladies and Gentlemen,

Good Morning! It is my great pleasure and honor to welcome you, on behalf of the International Telecommunication Union, to this ITU Regional Workshop on Frameworks for Cybersecurity and Critical Information Infrastructure Protection where I hope that all of you will have discussions of a most rewarding nature.

Let me first express our congratulations and best wishes to the newly established Ministry of Information and Communications of Vietnam and to HE Dr. Le Doan Hop for the appointment of His Excellency as its first Minister. Mr. Vice Minister, kindly extend our warm felicitations to HE, Minister Le Doan Hop. We would like to assure the leadership of the new Ministry of ITU's continued support and service as the Ministry undertakes its new and more challenging roles and responsibilities of looking after the telecommunications, posts, information technology, press and publication sectors in Vietnam.

Secondly, I would also like to thank the Ministry of Information and Communications of Vietnam for the active interest of Vietnam in the work of ITU on cybersecurity. We also appreciate the Ministry for the warm hospitality extended all the delegates since their arrival and the excellent hosting of this important workshop in this beautiful and historic city of Hanoi.

As we all know, confidence and security in the use of ICTs are fundamental in building an inclusive, secure and global information society, as acknowledged by the World Summit on Information Society (WSIS). However, threats have emerged that can seriously damage critical information infrastructures. Cyber-threats have become increasingly sophisticated since the early 1980s, when the first known case of a computer virus was reported. As recently as few years ago, the development of malware (including viruses, worms, and trojans) was a simple intellectual challenge to information technology experts to demonstrate their technical skills. Today, cybercrime has become an organized syndicate reaping financial rewards and using diverse tools to threaten different platforms in various countries. Thus, the WSIS, recognizing the real and significant risks posed by cyber-related threats and cybercrime, entrusted the ITU

to act as the main facilitator for the implementation of WSIS Action Line 5: Building confidence and security in the use of ICTs.

This workshop is the first in a series of regional events jointly organized by the ITU Telecommunication Development Sector and ITU Telecommunication Standardization Sector. It is directly linked to the ITU Asia Pacific Regional Initiative on “Strengthening the Collaboration between ITU-T and ITU-D” that was adopted at the World Telecommunication Development Conference in Doha, Qatar last year and is in response to a number of resolutions of the ITU Plenipotentiary Conference in 2006 and the World Telecommunication Standardization Assembly, in Florianopolis, Brazil in 2004. This event is also kindly supported by the Government of Australia and we wish to thank the Australian Department of Communication, Information Technology and the Arts for its cooperation and valuable support.

This workshop presents an excellent opportunity for sharing experiences and best practices on addressing the challenges faced by countries in the Asia Pacific region in developing frameworks for cybersecurity and critical information infrastructure protection as well as increasing awareness on the ITU-T Recommendations and activities relating to cybersecurity of both ITU-D and ITU-T.

For this workshop, we are very much pleased to have a line up of excellent speakers. I therefore would like to invite all of you to take advantage of the presence of these experts and your counterparts in other countries of the Asia Pacific region as well as other regions, to actively participate in all the sessions of the workshop by sharing your views and experiences and to raise any questions or issues you have regarding the subject. We have endeavored to design and conduct this workshop to hopefully benefit policy makers, regulators, service providers, operators and other stakeholders who are or would be involved in setting up or are implementing cybersecurity frameworks in their respective countries. Your active participation and contribution in this workshop will greatly contribute to its success.

I wish all of you a productive workshop and a wonderful stay here in Hanoi!

Thank you very much.