ITU-D's Activities in the Area of Cybersecurity and CIIP

ITU Regional Cybersecurity Forum for Europe and CIS

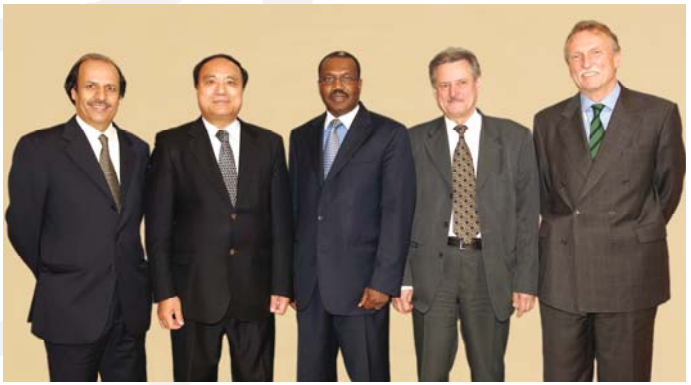
7-9 October 2008
Sofia, Bulgharia

Marco Obiso
ICT Applications and Cybersecurity Division
ITU Telecommunication Development Bureau (BDT)

International Telecommunication Union
Committed to connecting the world

ITU in brief

- Leading UN agency for information and communication technologies (ICT)
- The oldest UN agency (143 years)
- Global focal point for governments and the private sector. ITU's role in helping the world communicate spans 3 core sectors:
  - radiocommunication
  - standardization
  - development
  - ITU also organizes TELECOM events
- ITU is based in Geneva, Switzerland, and its membership includes 191 Member States and more than 700 Sector Members and Associates.
- Website: http://www.itu.int



ITU Mission & More

- **ITU's mission is to** enable the growth and sustained development of telecommunications and information networks, and to facilitate universal access so that people everywhere can participate in, and benefit from, the emerging information society and global economy.
- Instigator and manager of the World Summit on the Information Society (WSIS) held in two phases
  - Sole Facilitator for **WSIS Action Line C2** "Information and communication infrastructure" and **WSIS action Line C5** "Building confidence and security in the use of ICTs"

- **ITU** has been named as one of the **world's ten most enduring institutions** by US university scholars

ITU mission: bringing the benefits of ICT to all the world's inhabitants

- **Bridging the Digital Divide** by building information and communication infrastructure and promoting adequate capacity building;
- **Developing confidence in the use of cyberspace** through enhanced online security.
- **Strengthening emergency communications** for disaster prevention and mitigation;
- **Promoting the use of ICTs to combat climate change;**
- **Achieving equitable communication for everyone.**
- **ITU remains dedicated to helping the world communicate!**

Cybersecurity in ITU

- ITU's security standards cover a broad range of areas, including security principles for IMT (3G) networks, IP multimedia systems, NGN, network attacks, theft and denial of service, theft of identity, eavesdropping
- ITU is committed to building confidence and security in the use of ICT by creating an enabling environment through management of the international radio-frequency spectrum and the establishment of Recommendations
- As sole facilitator for WSIS Action Line C5, ITU launched the Global Cybersecurity Agenda (GCA) as a framework for dialogue and international cooperation to address global challenges in Cybersecurity. A High-Level Experts Group was established to advise the ITU Secretary-General on the complex issues surrounding cybersecurity.

ITU is engaged through in direct technical assistance to build capacity in Member States, particularly developing countries, to coordinate national strategies and protect network infrastructures from threats

ITU approach

ITU Strategic Framework
Global Cybersecurity Agenda (GCA)

- Inputs from ITU Sectors (ITU-T, ITU-R)
- Inputs from ITU-D (Study Groups)
- Inputs from membership and relevant players

↓

Elaboration of agreed strategies

↓

Implementation at national regional and international level

Special focus on Developing Countries

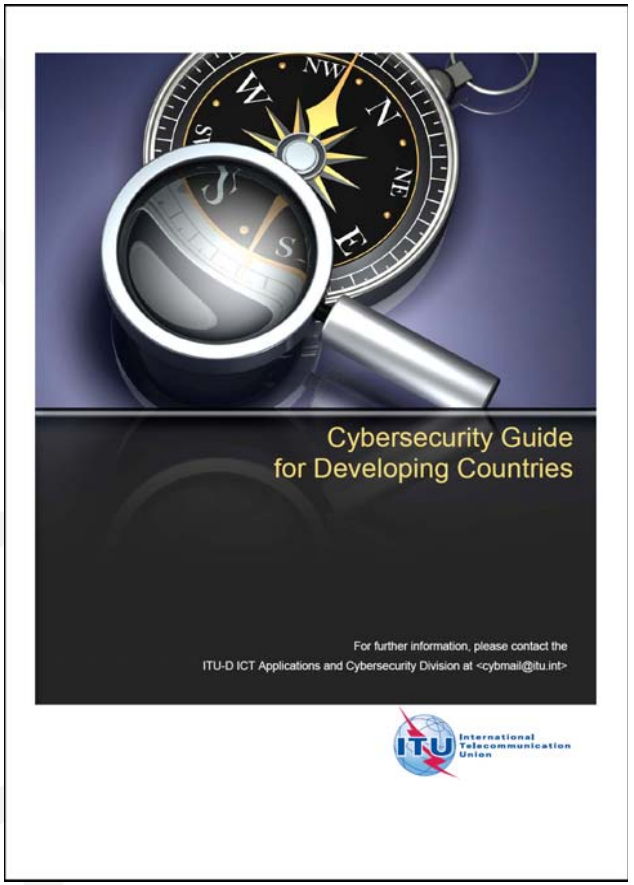
Multi-stakeholder approach

Assisting Developing Countries: Long History for ITU/BDT

- Projects based on PKI, including biometric authentication, smart cards, ITU-T X.509 digital certificates and digital signature techniques have been undertaken in *Barbados, Bhutan, Burkina Faso, Cambodia, Cameroon, Côte d'Ivoire, Georgia, Jamaica, Paraguay, Peru, Senegal, Turkey and Zambia*.
- Since 2002 ITU is organizing national and regional workshops and seminars addressing technology strategies for cybersecurity in a number of countries including *Azerbaijan, Cameroon, Chile (for the Mercosur states), Latvia, Mongolia, Pakistan, Paraguay, Peru, Romania, Seychelles, the Syrian Arab Republic and Uzbekistan*.

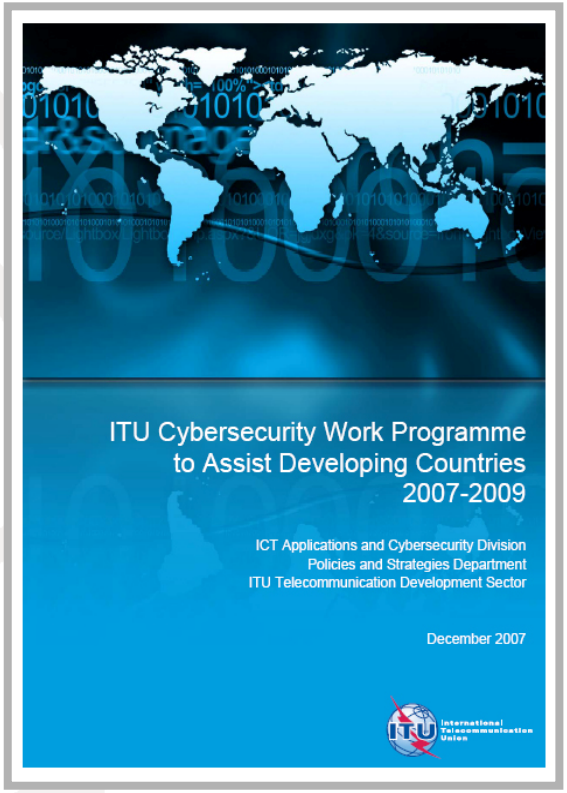
ITU Cybersecurity Guide for Developing Countries

- A basic and easy-to-use information tool to provide an initial understanding of Cybersecurity related dimensions, and solutions scenarios.
- It would facilitate the transfer of the necessary know-how to make the required step toward Cybersecurity.



ITU-D Cybersecurity Work Programme to Assist Developing Countries

- ITU-D Work Programme scopes a set of high level assistance activities on national strategies for cybersecurity and/or Critical Information Infrastructure Protection (CIIP)
- Also scopes detailed activities and initiatives planned to be implemented by the ITU-D together with Member States, private and public sector partners, and other regional and international organizations



- www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-cybersecurity-work-programme-developing-countries.pdf

Areas of activities

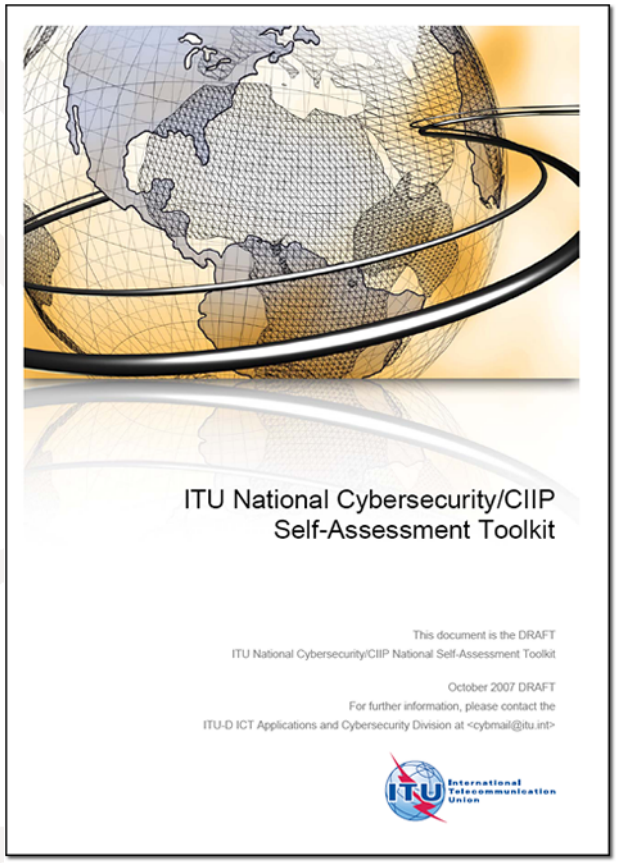
- Assistance related to Establishment of National Strategies and Capabilities for Cybersecurity and Critical Information Infrastructure Protection (CIIP)
- Assistance related to Establishment of appropriate Cybercrime Legislation and Enforcement Mechanisms
- Assistance related to establishment of Watch, Warning and Incident Response (WWIR) Capabilities
- Assistance related to Countering Spam and Related Threats
- Assistance in Bridging Security-Related Standardization Gap between Developing and Developed Countries
- Establishment of an ITU Cybersecurity/CIIP Directory and National Point of Contact Focal Database
- Cybersecurity Indicators
- Fostering International Cooperation Activities
- Information Sharing and Supporting the ITU Cybersecurity Gateway
- Outreach and Promotion of Related Activities

National Strategies/Capabilities for Cybersecurity and CIIP

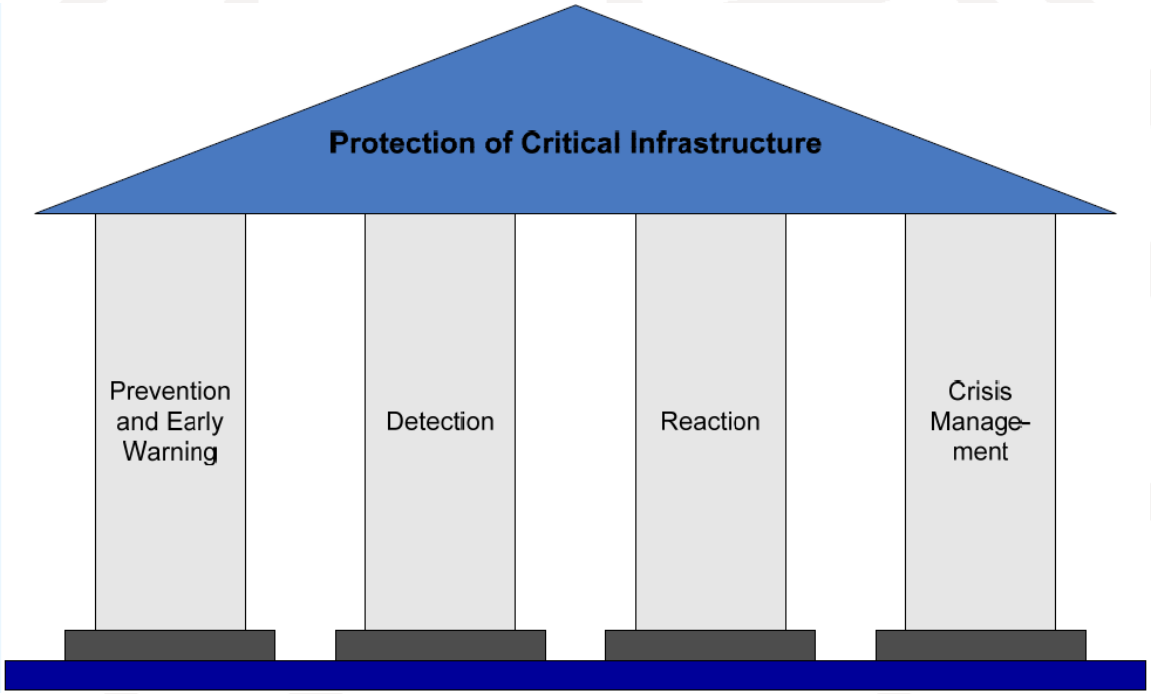
- National Cybersecurity/CIIP Readiness Self-Assessment Toolkit and related pilot projects
- Regional Cybersecurity Forums on Cybersecurity
  - 2007
    - August, Vietnam - October, Argentina - November, Cape Verde
  - 2008
    - February, Qatar – June, Australia - August. Zambia – October, Bulgaria
  - 2009
    - February, Caribbean – 2Q Tunisia, and others
- References:
  - www.itu.int/ITU-D/cyb/cybersecurity/projects/readiness.html
  - www.itu.int/ITU-D/cyb/cybersecurity/strategies.html
  - www.itu.int/ITU-D/cyb/events/

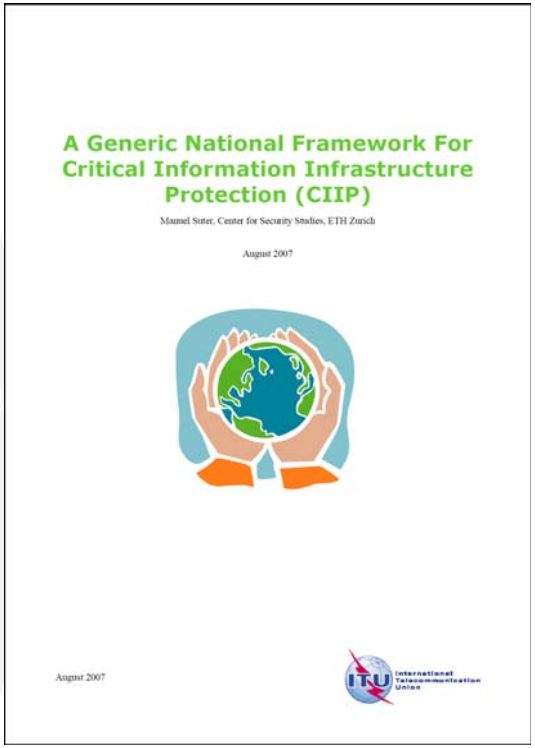
Self Assessment Tool

ITU National Cybersecurity/CIIP Self–Assessment Tool, to assist governments in examining existing national policies, procedures, norms, institutions and other elements necessary for formulating security strategies in an ever-changing ICT environment.



National Framework for CIIP





Establishment of Appropriate Cybercrime Legislation and Enforcement Mechanisms

- Regional Capacity Building Activities on Cybercrime Legislation and Enforcement
- Understanding Cybercrime Publication: undergoing editing.
- ITU Tool for Cybercrime Legislation (2009)
- References
  - www.itu.int/ITU-D/cyb/cybersecurity/legislation.html

Organizational Structures and Incident Management Capabilities

- Assistance to Developing Countries on the Establishment of Watch, Warning and Incident Response (WWIR) Capabilities
  - Coordination and cooperation with key players (FIRST)
  - e.g. facilitate the establishment of a Pacific CERT (2009)
- Computer Security Incident Response Team (CSIRT)
  - CSIRT survey
  - CSIRT toolkit
- Inventory of Watch, Warning and Incident Response Capabilities by Region
- References
  - www.itu.int/ITU-D/cyb/cybersecurity/wwir.html

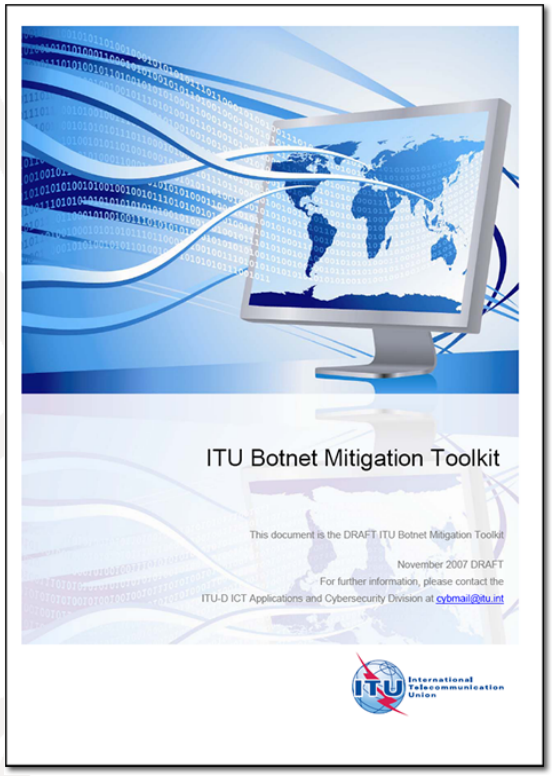
Countering Spam and Related Threats

- Survey on Anti-Spam Legislation Worldwide (underway)
- Botnet Mitigation Toolkit for Developing Countries
  - Pilot Projects for Implementation of Toolkit (Malaysia)
- Study on Financial Aspects of Spam and Malware (with ITU-T Study Group 3)
- Translation of Message Anti-Abuse Working Group Best Practices Docs
  - Code of Conduct
  - MAAWG - Managing Port25
  - BIAC-MAAWG Best Practices Expansion Document
  - Anti-Phishing Best Practices for ISPs and Mailbox Providers
  - MAAWG Sender BCP Version 1.1 & Executive Summary

- References
  - www.itu.int/ITU-D/cyb/cybersecurity/spam.html

ITU Botnet Mitigation Package

- Framework for national botnet related policy, regulation and enforcement
- Multi-stakeholder international cooperation and outreach
  - Phase 1 (2007): Downloadable toolkit/guidelines for ITU Member States
  - Phase 2 (2008/2009): Targeted national/regional assistance initiatives



ITU Study on Financial Aspects of Network Security: Malware and Spam

- Malware and spam are converging: spam is used to expand and sustain botnets, which are, in turn, used to send spam
- Negative and positive financial effects
  - Costs for individuals, organizations, nations
  - Benefits for legal but also illegal players
- This ITU study aims to document the state of knowledge of these financial aspects of cybersecurity

More Information

- ITU-D ICT Applications and Cybersecurity Division:
  - www.itu.int/itu-d/cyb/
- ITU-D Cybersecurity Overview:
  - www.itu.int/itu-d/cyb/cybersecurity/
- ITU National Cybersecurity/CIIP Self-Assessment Toolkit:
  - www.itu.int/ITU-D/cyb/cybersecurity/projects/readiness.html
- ITU-D Cybersecurity Work Programme to Assist Developing Countries:
  - www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-cybersecurity-work-programme-developing-countries.pdf
- Regional Cybersecurity Forums:
  - www.itu.int/ITU-D/cyb/events/
- Botnet Mitigation Toolkit:
  - www.itu.int/ITU-D/cyb/cybersecurity/projects/botnet.html
- Information on ITU Global Cybersecurity Agenda (GCA):
  - www.itu.int/gca/
- Details on Cybersecurity Activities Undertaken by ITU:
  - www.itu.int/cybersecurity/

Thank you for your attention!

International Telecommunication Union