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

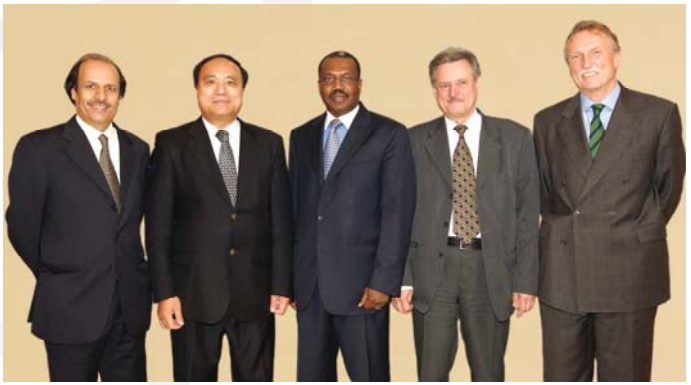
ITU Regional Cybersecurity Forum for Eastern and Southern Africa

25-28 August 2008
Lusaka, Zambia

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

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

Cybersecurity in ICT Development

Background and Mandate

- ITU Plenipotentiary and World Telecommunication Development conferences related resolutions (Res. 130, Res. 45)
- Cybersecurity part of Programme 3 managed by ITU-D ICT Applications and Cybersecurity Division
- ITU-D Study Group 1 Question 22/1

Cybersecurity in ITU-D

- ITU-D Programme 3 Cybersecurity Work Programme to Assist Developing Countries
- ITU-D Study Group 1 Question 22/1: Securing information and communication networks: Best practices for developing a culture of cybersecurity

Synergies exist between the activities under these two pillars and with other ITU Cybersecurity related programmes and initiatives

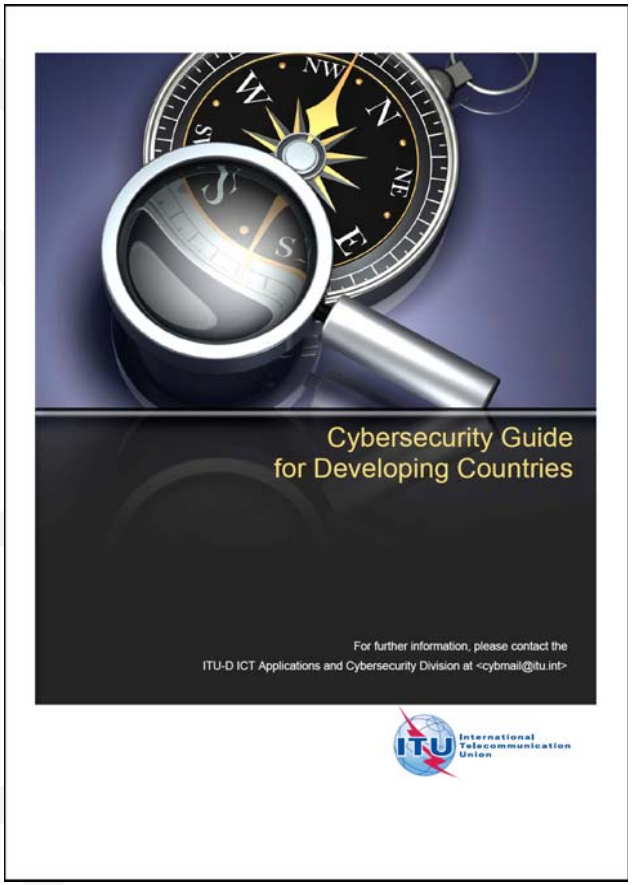
For more info, see www.itu.int/ITU-D/cyb/

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, Bulgaria, 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*.

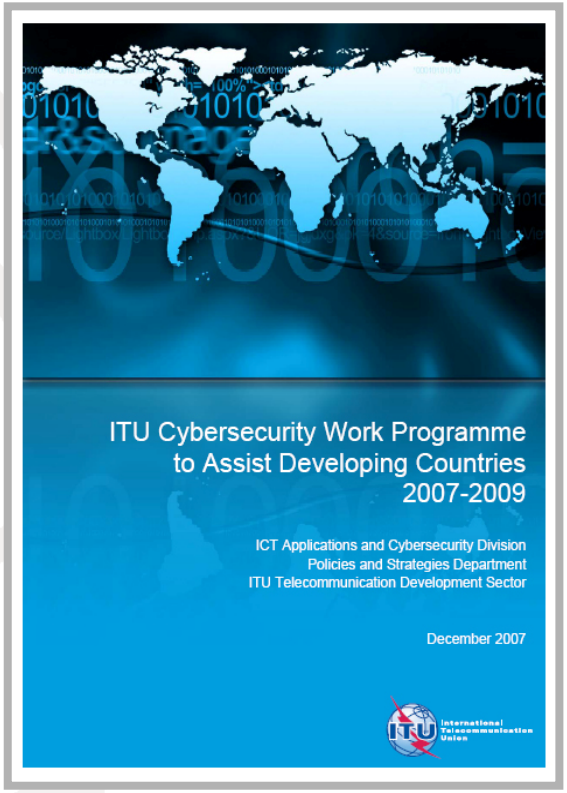
ITU Cybersecurity Guide for Developing Countries

- 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

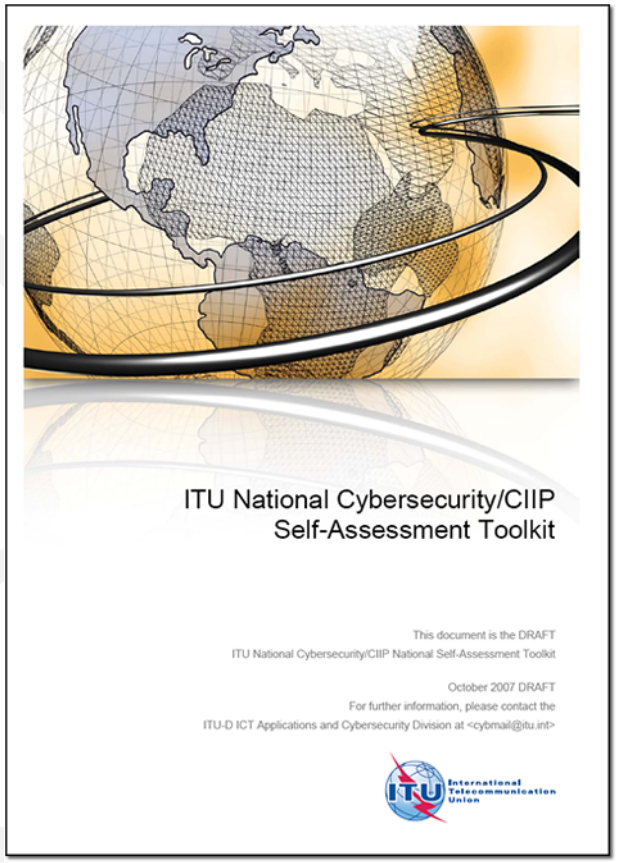
- Assistance related to Establishment of National Strategies and Capabilities for Cybersecurity and Critical Information Infrastructure Protection (CIIP)
- Assistance related to Establishment of appropriate Cybercrime Legislation and Enforcement Mechanisms
- Assistance related to establishment of Watch, 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

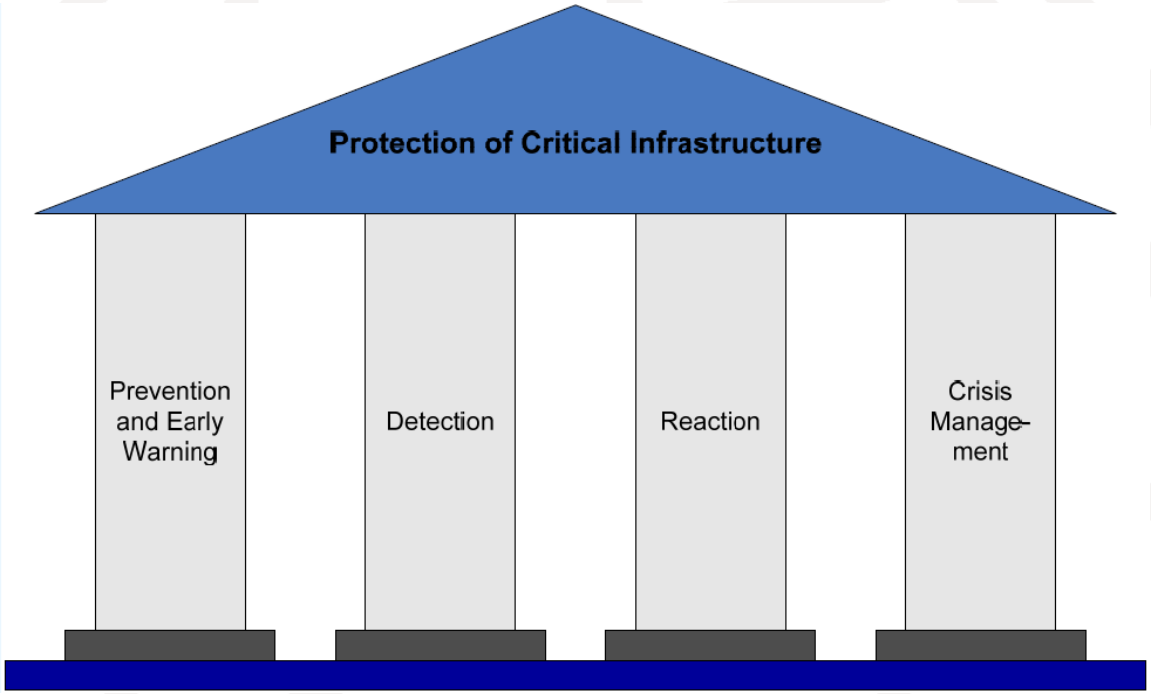
- National Cybersecurity/CIIP Readiness Self-Assessment Toolkit and related pilot projects
- Regional Cybersecurity Forums on Cybersecurity
  - 2007
    - August, Vietnam - October, Argentina - November, Cape Verde
  - 2008
    - February, Qatar – June, Australia - August. Zambia – October, Bulgaria
  - 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/

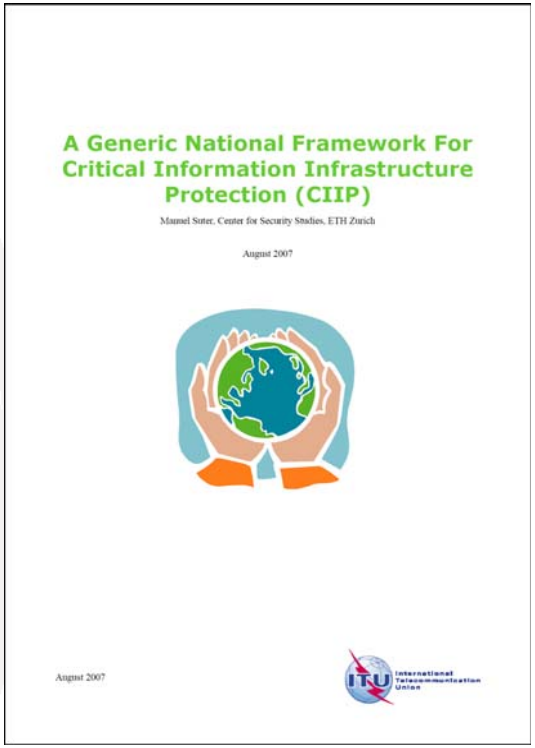
Self Assessment Toolkit

ITU National Cybersecurity/CIIP Self–Assessment Toolkit, 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





ITU-D ICT Applications and Cybersecurity (CYB) - Windows Internet Explorer

http://www.itu.int/ITU-D/cyb/cybersecurity/strategies.html

ITU-D ICT Applications and Cybersecurity (CYB)

International Telecommunication Union

عربي | 中文 | Español | Français | Русский

Home : ITU-D : ICT Applications and Cybersecurity Division : Cybersecurity

Search

Home | ITU Sectors | Newsroom | Events | Publications | About Us

Back to CYB

CYB Activities

- Cybersecurity
- E-Strategies
- ICT Applications
- Internet and IP Networks
- Telecentres

General Information

- Events
- Newslog
- Publications
- Contact CYB
- ITU-D Study Groups
- ITU-D Main Site

Visitor locations

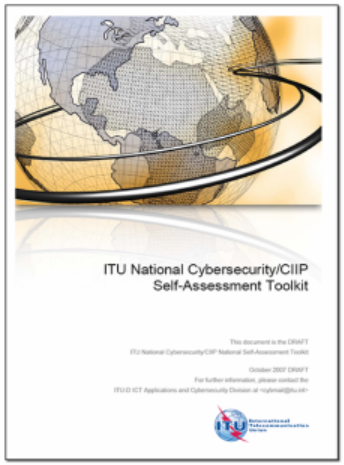
ClustrMaps Click to see

National Strategies for Cybersecurity and Critical Information Infrastructure Protection (CIIP)

Modern societies have a growing dependency on information and communication technologies that are globally interconnected. However, this interconnectivity also creates interdependencies and risks that need to be managed at national, regional and international levels. Enhancing cybersecurity and protecting critical information infrastructures are essential to each nation's security and economic well-being.

At the national level, this is a shared responsibility requiring coordinated action related to the prevention, preparation, response, and recovery from incidents on the part of government authorities, the private sector and citizens. At the regional and international level, this entails cooperation and coordination with relevant partners. The formulation and implementation of a national framework for cybersecurity and critical information infrastructure protection (CIIP) requires a comprehensive approach.

Promoting National Strategies



ITU-D Study Group Question 22/1

- Question 22/1: Securing information and communication networks: Best practices for developing a culture of cybersecurity
- Contributions to Rapporteurs' Group Question Q22/1 (*TIES login and password required*)
- Contributions to Study Group Question Q22/1 (*TIES login and password required*)
- ITU Study Group Q.22/1 Report on Best Practices for a National Approach to Cybersecurity: a Management Framework for Organizing National Cybersecurity Efforts

ITU National Cybersecurity/CIIP Self-Assessment Toolkit

- Background Information and Documents
- Project Overview (September 2007)

Regional Workshops on Frameworks for Cybersecurity and CIIP

- 18-21 February 2008 (Doha, Qatar): Regional Workshop on Frameworks for Cybersecurity and Critical Information Infrastructure Protection (CIIP) and Cybersecurity Forensics Workshop
- 27-29 November 2007 (Praia, Cape Verde): West Africa Workshop on Policy and Regulatory Frameworks for Cybersecurity and CIIP

Newslog

- ITU Paper: Study Group Q.22/1 Report on Best Practices for a National Approach to Cybersecurity
- Presentation: ICTs and e-Environment - Overview of BDT Scoping Study for Developing Countries

[Browse CYB News Feeds]

Resources

ITU Cybersecurity Gateway

The ICT Eye

[More ITU-D resources]

Publications

http://www.itu.int/cybersecurity/gateway/

Local intranet | 100%

Establishment of Appropriate Cybercrime Legislation and Enforcement Mechanisms

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

International Telecommunication Union

Back to CYB

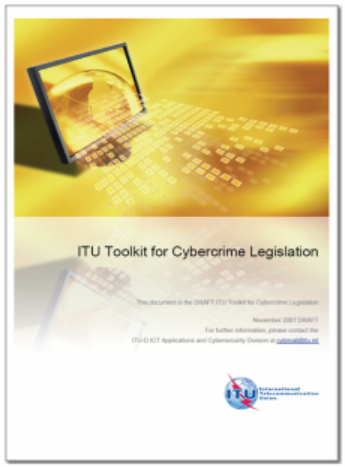
CYB Activities
- Cybersecurity
- E-Strategies
- ICT Applications
- Internet and IP Networks
- Telecentres

General Information
- Events
- Newslog
- Publications
- Contact CYB
- ITU-D Study Groups
- ITU-D Main Site

Legislation and Enforcement

An integral component of any national cybersecurity strategy is the adoption of appropriate legislation against the misuse of ICTs for criminal or other purposes, including activities intended to affect the integrity of national critical information infrastructures. As threats can originate anywhere around the globe, the challenges are inherently international in scope and it is desirable to harmonize legislative norms as much as possible to facilitate regional and international cooperation. Links to some related activities and resources can be found below.

About Cybercrime Legislation and Law Enforcement



ITU Toolkit for Cybercrime Legislation

- Project Background Information and Resources
- Project Overview (October 2007)

Background Resources

- Council of Europe (COE): Convention on Cybercrime
- Council of Europe Survey of Countries' Cybercrime Legislation
- Cybercrimelaw.net: A Survey of Cybercrime Laws Worldwide
- Interpol: Information Technology Crime Resources
- Microsoft: Asia Pacific Legislative Analysis: Current and Pending Online Safety and Cybercrime Laws, 2007
- Models for Cyber Legislation in Economic and Social Commission for Western Asia (ESCWA) Member Countries, 2007
- US Department of Justice: Manual on Prosecuting Computer Crime (Chapter 1 - Computer Fraud and Abuse Act), 2007
- US Secret Service: Best Practices for Seizing Electronic Evidence
- ITU Cybersecurity Gateway: Background material related to harmonization of national legal approaches, international legal coordination and enforcement

UN Cybercrime Legislation and Enforcement Specific Resolutions

- UN Resolutions 55/63 (2000) and 56/121 (2001): Combating the Criminal Misuse of Information Technologies
- UN Resolutions 57/239 (2002) and 58/199 (2004): Creation of a global culture of cybersecurity and the protection of critical information infrastructures

Newslog

- ITU Paper: Study Group Q.22/1 Report on Best Practices for a National Approach to Cybersecurity
- Presentation: ICTs and e-Environment - Overview of BDT Scoping Study for Developing Countries

[Browse CYB News Feeds]

Resources

ITU Cybersecurity Gateway

The ICT Eye

[More ITU-D resources]

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

Watch, Warning and Incident Response (WWIR)

A key activity for addressing cybersecurity at the national level pertains to preparing for, detecting, managing, and responding to cyber incidents through establishment of watch, warning and incident response capabilities. Effective incident management requires consideration of funding, human resources, training, technological capability, government and private sector relationships, and legal requirements. Collaboration at all levels of government and with the private sector, academia, regional and international organizations, is necessary to raise awareness of potential attacks and steps toward remediation. Links to some related activities and resources can be found below.

More on Watch, Warning and Incident Response

Background Resources

- CERT/CC: The CERT Action List for Developing a Computer Security Incident Response Team (CSIRT)
- CERT/CC: Handbook for Computer Security Incident Response Teams (CSIRTs) (Rev. 2003)
- CERT/CC: CERT FAQ, CERT/CC presentations, other CERT/CC publications
- CERT/CC: Security vulnerabilities and fixes
- CERT/CC Virtual Training Environment (VTE)
- Forum of Incident Response and Security Teams (FIRST) resources
- European CSIRT Network resources
- European Government CERTs (EGC) Group
- Dutch Belnet CERT resources
- TERENA TF-CSIRT resources (task force involves CSIRTs/CERTs from all over Europe)
- ENISA: Inventory of CERT activities in Europe, 2006
- Regional Asia Pacific Computer Emergency Response Team (APCERT) resources

CSIRTs/CERTs/WARPs

Computer Security Incident Response Teams (CSIRTs), Computer Emergency Response Teams (CERTs), or Warning, Advice and Reporting Points (WARPs) are coordination centers dealing with security problems and, as the names would suggest, responding to major incidents. With these teams available, it is possible to mitigate and prevent major incidents.

In addition to reactive services, such as incident response, the CSIRTs and CERTs nowadays also often provide their customers with a variety of other security services, this includes: alerts and warnings, advisories, technical assistance and security-related training.

Information Resources

- ENISA: CSIRT Step-by-Step guide, 2006
- CPNI, United Kingdom: The WARP Toolbox
- GOVCERT.nl, The Netherlands: CSIRT in a Box
- Training resource for incident response teams organized by TERENA's TF-CSIRT and funded by the European Commission
- Clearing House for Incident Handling Tools (CHIHT) resources (includes listing of incident handling tools)

Newslog

- 19 September 2007: ENISA / CERT/CC Workshop on Mitigation of Massive Cyberattacks
- ITU News: Cybersecurity Watch September Edition

[Browse CYB News Feeds]

Resources

ITU Cybersecurity Gateway

The ICT Eye

[More ITU-D resources]

Publications

- ITU and ETH Zurich: A Generic National Framework for Critical

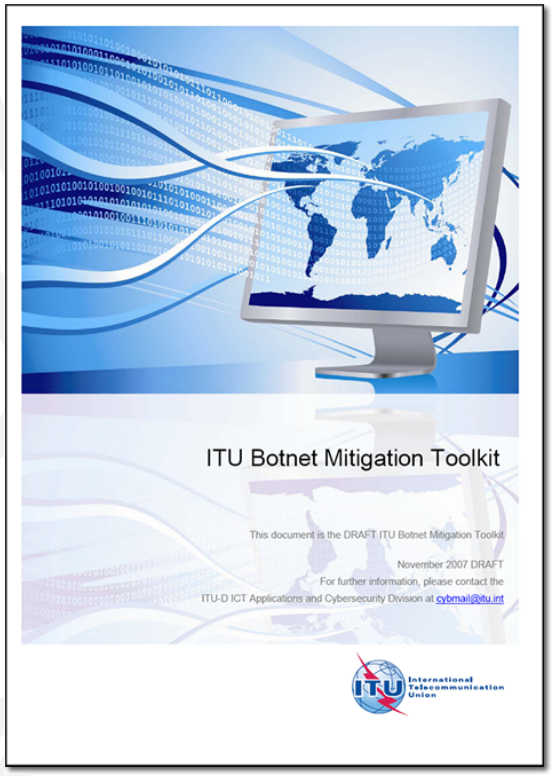
Countering Spam and Related Threats

- 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

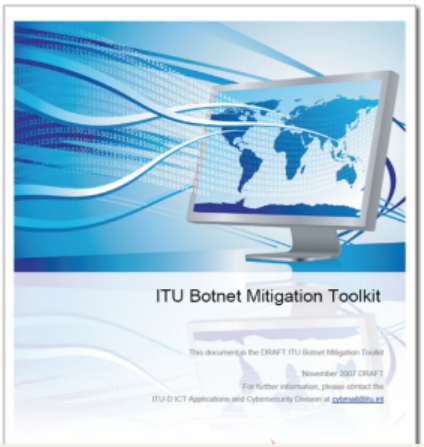
- Malware and spam are converging: spam is used to expand and sustain botnets, which are, in turn, used to send spam
- Negative and positive financial effects
  - Costs for individuals, organizations, nations
  - Benefits for legal but also illegal players
- This ITU study aims to document the state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

Countering Spam and Related Threats

Spamming is the abuse of electronic messaging systems to send unsolicited bulk messages, which are generally undesired. While the most widely recognized form of spam is email spam, the term is applied to similar abuses in other media: instant messaging spam, Usenet newsgroup spam, Web search engine spam, spam in blogs, mobile phone messaging spam, internet forum spam and junk fax transmissions. Spamming is economically viable because advertisers have no operating costs beyond the management of mailing lists, and it is difficult to hold senders accountable for their mass mailings. Because the barrier to entry is so low, spammers are numerous, and the volume of unsolicited mail has become very high and represents almost 90 per cent of all email.

The costs, such as lost productivity and fraud, are borne by the public and by Internet service providers, which have been forced to add extra capacity to cope with the deluge. Spam is particularly problematic for developing countries who have thin pipe connectivity to the Internet backbone which becomes clogged with unwanted traffic. Spam is also the primary attack vector for delivery of viruses and forms of malware. Links to some of ITU's spam related activities and resources can be found below.

ITU Spam Related Activities



ITU-D Study Group Question 22/1

- Question 22/1 Definition: Securing information and communication networks: Best practices for developing a culture of cybersecurity
- Contributions to Rapporteurs Group Question Q22/1 (*TIES login and password required*)
- 17 September 2007 (Geneva, Switzerland): Workshop on Frameworks for National Action: Cybersecurity and Critical Information Infrastructure Protection

ITU Spam Related Resolutions

- ITU Plenipotentiary Resolution 130: Strengthening the role of ITU in building confidence and security in the use of information and communication technologies (Antalya, 2006)
- ITU Plenipotentiary Resolution 149: Study of definitions and terminology relating to building confidence and security in the use of information and communication technologies (Antalya, 2006)

Spam Newslog

- Infiltrating the Phishing Underground
- 2M New Websites a Year Compromised To Serve Malware

[More Spam Related News Feeds]

Related Resources

OnGuard Online YOUR SAFETY NET TM
Tips and Tools at OnGuardOnline.gov

Anti Spam Video
From antispam.br

GOVCERT.NL's
Botnet Movie

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/
- Study Group Q22/1: Report On Best Practices For A National Approach To Cybersecurity: A Management Framework For Organizing National Cybersecurity Efforts:
  - www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-draft-cybersecurity-framework.pdf
- 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