

Overview of ITU-D Activities Related to Cybersecurity and Critical Information Infrastructure Protection

West Africa Workshop on Policy and Regulatory
Frameworks for Cybersecurity and Critical
Information Infrastructure Protection (CIIP)

Praia, Cape Verde

16-18 October 2007

Robert Shaw

Head, ICT Applications and Cybersecurity Division

Policies and Strategies Department

ITU Telecommunication Development Sector

.....

Introduction to ITU

- International organization where governments and private sector coordinate global telecom networks and services
- Founded in 1865, it is oldest specialized agency of the UN system
- 191 Member States, 780 Sector Members & Sector Associates
- Headquarters Geneva, 11 regional offices, 760 staff / 80 nationalities

ITU Mission & More

- Maintain and extend international cooperation in telecommunications
- Technical and policy assistance to developing countries
- To harmonize actions of Member States and promote cooperation between Member States and Sector Members
- Instigator and manager of the **World Summit on the Information Society (WSIS)** held in two phases
- ITU has been named as one of the world's ten most enduring institutions by US university scholars

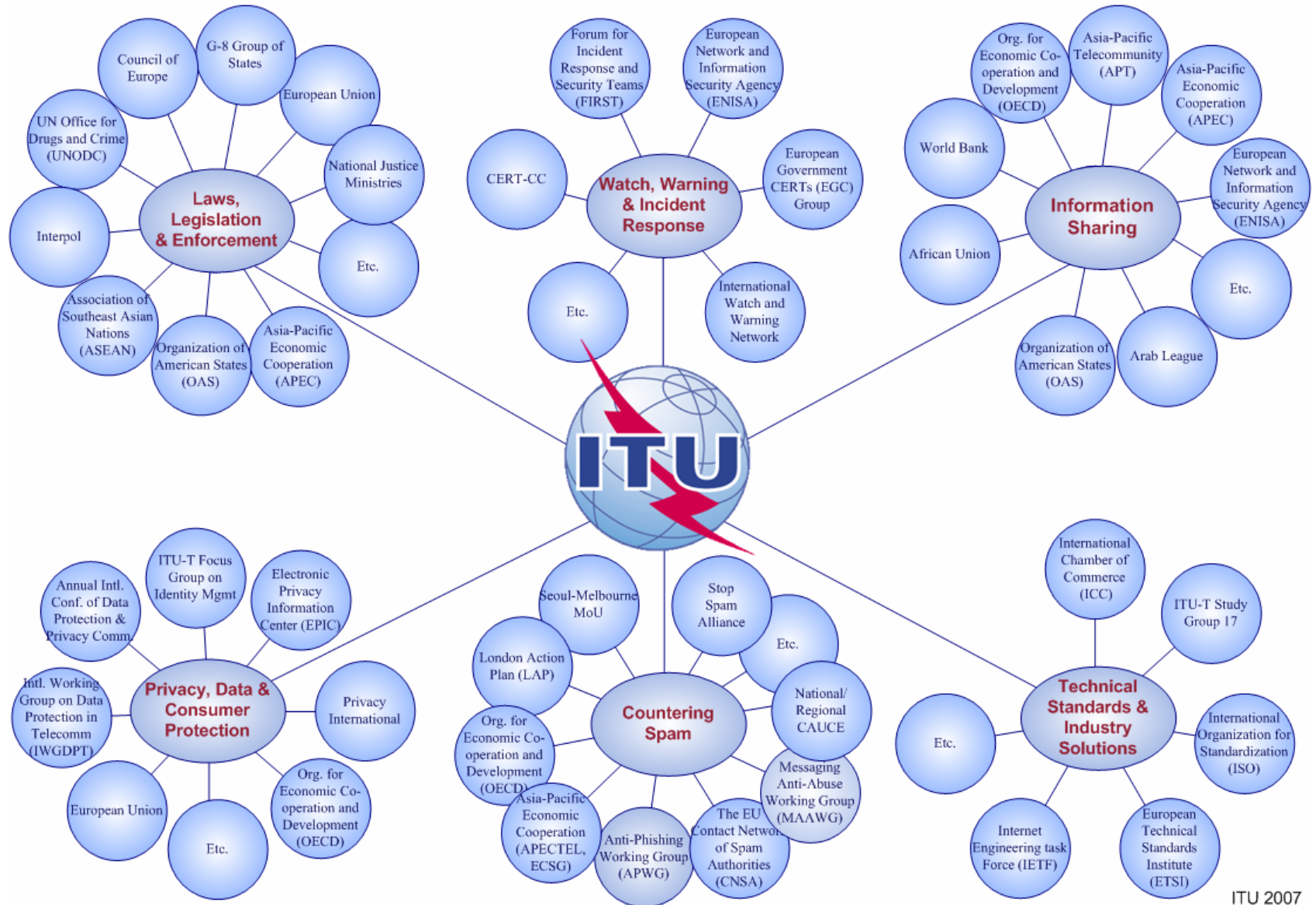


Setting the Context

- In the 21st century, growing dependency on information and communications technologies (ICTs) that span the globe;
- Rapid growth in ICTs and dependencies led to shift in perception of cybersecurity threats in mid-1990s;
- Growing linkage of cybersecurity and critical information infrastructure protection (CIIP);
- Number of countries began assessment of threats, vulnerabilities and explored mechanisms to redress them;
- But most countries have not formulated or implemented a national strategy for cybersecurity or Critical Information Infrastructure Protection (CIIP) programme;
- In parallel with national consideration, move to international political agenda.



Many Actors in International Cybersecurity/CIIP Ecosystem

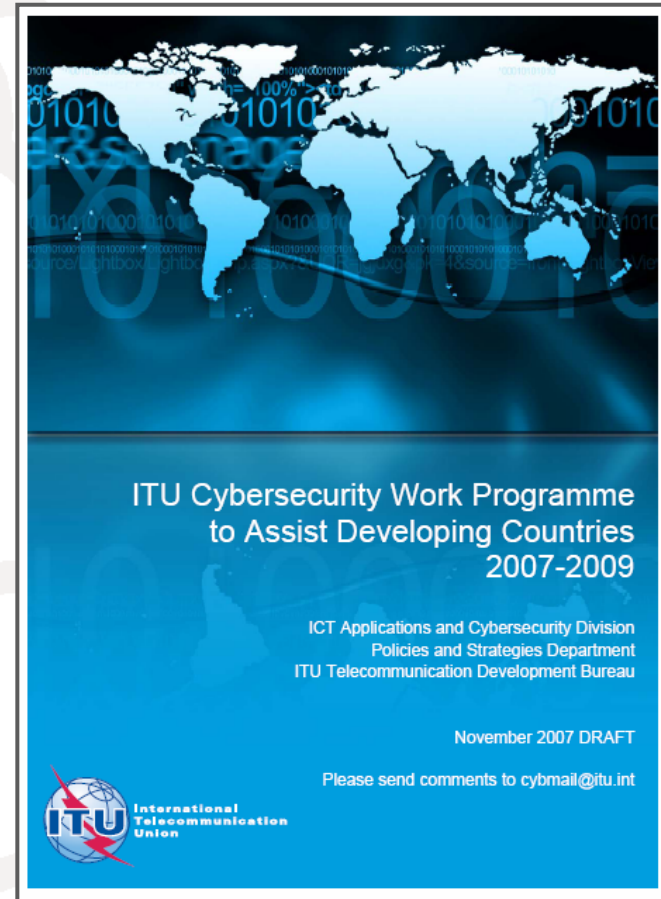


ITU Development Sector Role

- ITU Resolution 130: Strengthening the role of ITU in building confidence and security in the use of information and communication technologies (Antalya, 2006);
- From World Telecommunication Development Conference (Doha, 2006):
 - ITU-D Study Group 1 Question 22/1
 - Cybersecurity is priority activity in Programme 3 activities, managed by [ITU-D ICT Applications and Cybersecurity Division](#)

Key Activities Underway in ITU-D

- ITU-D Study Group 1
Question 22/1: *Securing information and communication networks: Best practices for developing a culture of cybersecurity*
 - Outlines *Framework for Organizing a National Approach to Cybersecurity*
- ITU Cybersecurity Work Programme to Assist Developing Countries
- Close synergies between these two activities

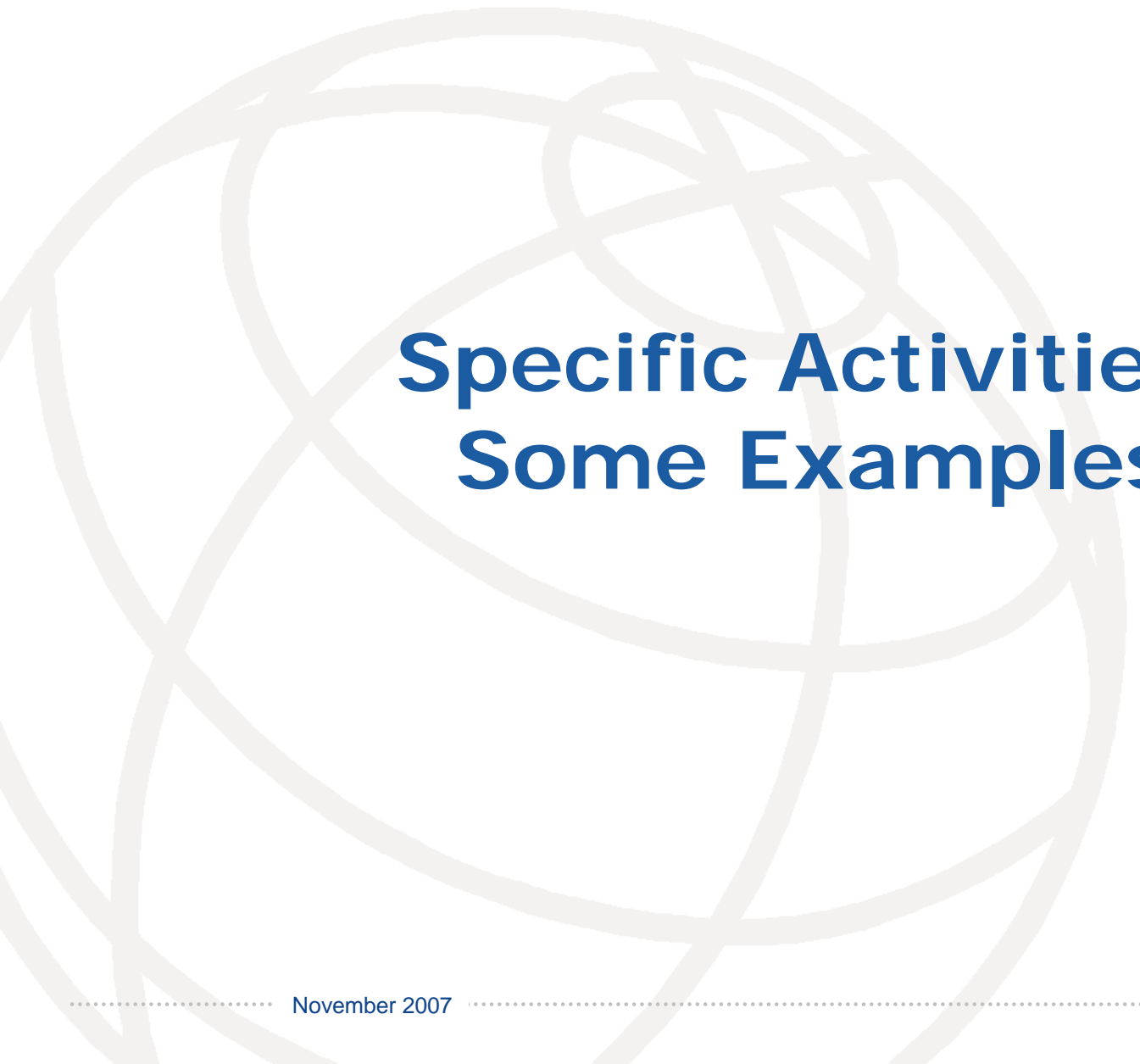


www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-cybersecurity-work-programme-developing-countries.pdf

Cybersecurity Work Programme to Assist Developing Countries: High Level Elements

- 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
- Project on Enhancing Cybersecurity and Combatting Spam
- Establishment of an ITU Cybersecurity/CIIP Directory, Contact Database and Who's Who Publication
- Cybersecurity Indicators
- Fostering Regional Cooperation Activities
- Information Sharing and Supporting the ITU Cybersecurity Gateway
- Outreach and Promotion of Related Activities

<http://www.itu.int/itu-d/cyb/cybersecurity/>



Specific Activities: Some Examples

Establishment of National Strategies/Capabilities for Cybersecurity and Critical Information Infrastructure Protection (CIIP)

- Best Practices in the Establishment of National Frameworks for Cybersecurity and CIIP
- National Cybersecurity/CIIP Readiness Self-Assessment Toolkit
 - Pilot tests in selected countries
- Regional Workshops on Frameworks for Cybersecurity and CIIP
- Online Experts Forum to Help Developing Countries Develop Capacity
- Toolkit for Promoting a Culture of Cybersecurity
- Online Training Modules for Cybersecurity Awareness and Solutions

- References:
 - <http://www.itu.int/ITU-D/cyb/cybersecurity/projects/readiness.html>
 - <http://www.itu.int/ITU-D/cyb/cybersecurity/strategies.html>
 - <http://www.itu.int/ITU-D/cyb/events/>

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

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

National Strategies for Cybersecurity and 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

Regional Workshops on Frameworks for Cybersecurity and CIIP

- 27-29 November 2007 (Praia, Cape Verde): [West Africa Workshop on Strategies for Cybersecurity and Critical Information Infrastructure Protection](#)
- 29-31 October 2007 (Damascus, Syria): [Regional Workshop on E-Signatures and Identity Management](#)
- 16-18 October 2007 (Buenos Aires, Argentina): [Regional Workshop on Frameworks for Cybersecurity and Critical Information Infrastructure Protection](#)
- 17 September 2007 (Geneva, Switzerland): [Workshop on Frameworks for National Action: Cybersecurity and Critical Information Infrastructure Protection](#)
- 28-31 August 2007 (Hanoi, Vietnam): [Regional Workshop on Frameworks for Cybersecurity and Critical Information Infrastructure Protection](#)

[See more events...]

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 \(TIES login and password required\)](#)
- [Contributions to Study 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 National Cybersecurity/CIIP Self-Assessment Toolkit

[Project Overview \(September 2007\)](#)

Papers and Publications

[ITU and ETH Zurich: A Generic National Framework for Critical Information Infrastructure Protection, 2007](#)

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]

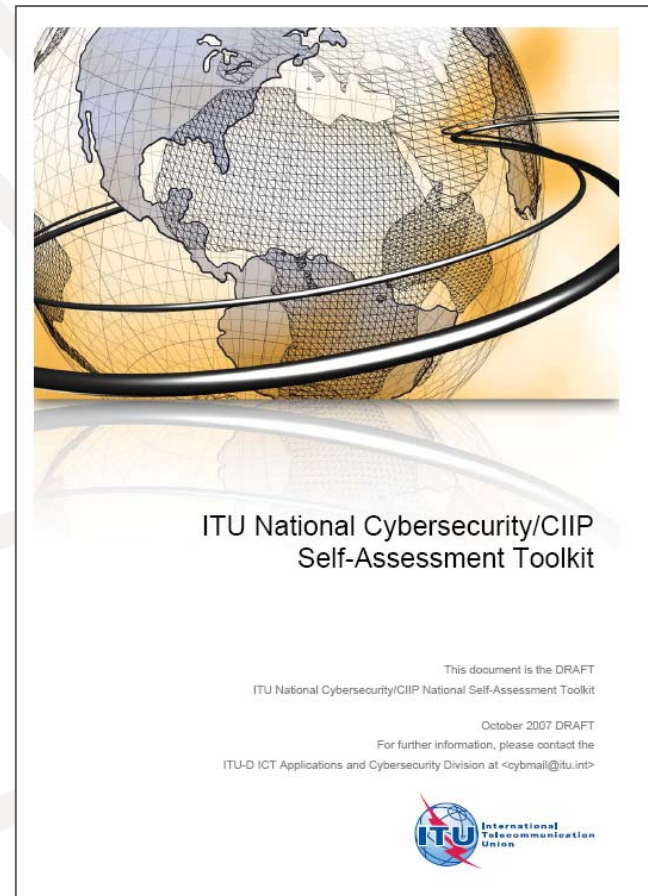
Publications

- [ITU and ETH Zurich: A Generic National Framework for Critical Information Infrastructure Protection, 2007](#)



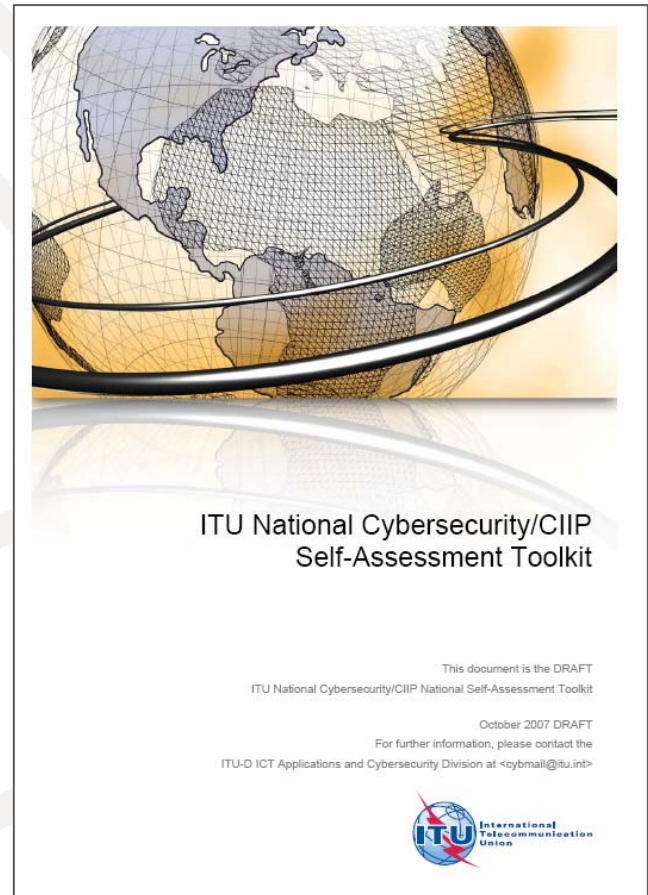
ITU National Cybersecurity/CIIP Self-Assessment Toolkit

- Based on Q.22/1 Framework Best Practice Documents
- Focused on national management and policy level
- Intended to assist national administrations to:
 - understand existing approach
 - compare to best practices
 - identify areas for attention
 - prioritize national efforts



ITU National Cybersecurity/CIIP Self-Assessment Toolkit cont'd

- Includes Annex on *Deterring Cybercrime: Substantive, Procedural and Mutual Assistance Law Baseline Survey*
- Intended to assist national authorities to review their domestic situation related to goals and actions identified in:
 - UN [Resolutions 55/63](#) (2000) and [56/121](#) (2001): Combating the Criminal Misuse of Information Technologies
 - [Council of Europe's Convention on Cybercrime](#) (2001)
- Adopted from work in APEC-TEL





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

Search

Back to CYB

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

CYB Activities

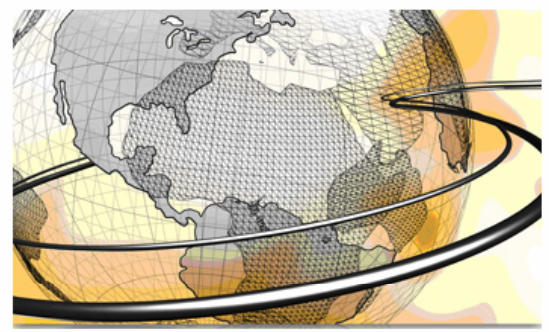
- Cybersecurity
- E-Strategies
- ICT Applications
- Internet and IP Networks
- Telecentres

General Information

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



ITU National Cybersecurity/CIIP Self-Assessment Toolkit



The ITU National Cybersecurity/CIIP Self Assessment Toolkit is based on studies underway in the ITU Telecommunication Development Sector's Study Group 1, Question 22/1: *Securing information and communication networks: best practices for developing a culture of cybersecurity*. This activity calls for ITU Member States and Sector Members to create a report on national best practices in the field of cybersecurity. Links to more information on Question 22/1 activities can be found on the main ITU-D [cybersecurity website](#).

The toolkit is intended to assist national governments in examining their existing national policies, procedures, norms, institutions, and relationships in light of national needs to enhance cybersecurity and address critical

information infrastructure protection.

This toolkit is directed to leadership at the policy and management levels of government, and addresses the policies, institutional framework, and relationships for cybersecurity. It seeks to produce a snapshot of the current state of national policy and capability, of institutions and institutional relationships, of personnel and expertise, of relationships among government entities and relationships among government, industry and other private sector entities.

The draft toolkit includes an Annex on *Deterring Cybercrime: Substantive, Procedural and Mutual Assistance Law Baseline Survey* intended to assist national authorities to review their domestic situation related to the goals and actions identified in United Nations [Resolutions 55/63](#) (2000) and [56/121](#) (2001) on Combating the Criminal Misuse of Information Technologies and the [Council of Europe's Convention on Cybercrime](#) (2001).

- [Powerpoint Project Overview](#) (October 2007)
- [Draft Background Information for National Pilot Tests](#) (October 2007)
- [Draft ITU National Cybersecurity/CIIP Self-Assessment Toolkit](#) (October 2007)
- [Draft Implementation Matrix Work Booklet \(Word, PDF\)](#) (October 2007)

Newslog

- 28-30 November 2007: ITU Regional Workshop on ICT Applications for Rural Communication Development (Bali, Indonesia)
 - ITU Project: ITU Botnet Mitigation Toolkit
- [Browse CYB News Feeds]

Publications

- ITU and ETH Zurich: A Generic National Framework for Critical Information Infrastructure Protection (CIIP), 2007
- Cybersecurity Guide for Developing Countries (English), 2007. Non-finalized versions are also available in [عربي](#), [中文](#), [Français](#), [Русский](#) and [Español](#). NB: A printed copy of this publication is available on request.
- Cybersecurity Guide for Developing Countries (English, Français), 2006
- Research on Legislation in Data Privacy, Security and the Prevention of Cybercrime (English), 2006
- ITU Cybersecurity Watch - September 2007 Edition
- ITU Cybersecurity Watch - May 2007 Edition

Establishment of Appropriate Cybercrime Legislation and Enforcement Mechanisms

- Regional Capacity Building Activities on Cybercrime Legislation and Enforcement
- Cybercrime Publication: early 2008
- Model Cybercrime Law Toolkit (early 2008)
- Cybersecurity Module in the ITU/InfoDev ICT Regulation Toolkit

- References
 - <http://www.itu.int/ITU-D/cyb/cybersecurity/legislation.html>



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

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

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

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

Background Resources

- Council of Europe (COE): [Convention on Cybercrime](#)
- Cybercrimelaw.net: [A Survey of Cybercrime Laws Worldwide](#)
- Interpol: [Information Technology Crime Resources](#)
- US Department of Justice: [Manual on Prosecuting Computer Crime \(Chapter 1 - Computer Fraud and Abuse Act\), 2007](#)
- 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

Ongoing and Planned Projects

Regional Workshops and Capacity Building Activities Related to Cybercrime Legislation and Enforcement

In order to increase awareness among ITU Member States on the importance of cybersecurity legislation and law enforcement, a number of regional capacity building activities and workshops on cybercrime legislation and enforcement are currently being planned. Partnerships with the [Council of Europe](#), [UNODC](#), [Interpol](#), and National Departments of Justice have been established to aid in the implementation of these and related activities. [\[See more information...\]](#)

- [Publication on Cybersecurity for Developing Countries to include a Cybercrime Chapter](#)

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



Toolkit for Model Cybercrime Legislation

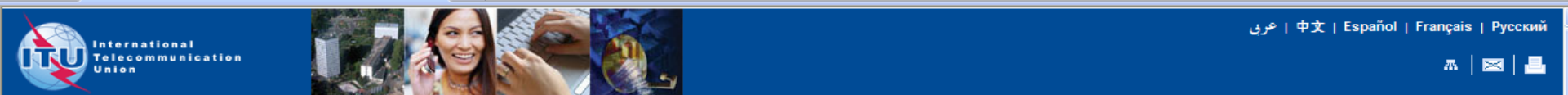
- Representing one of five elements Q22/1, deterring cybercrime is an integral component of a national cybersecurity/CIIP strategy
- Toolkit for Model Cybercrime Legislation aims to provide countries with model legislation that can assist in establishment of a legislative framework to deter cybercrime;
- Development of toolkit undertaken by multidisciplinary international group of experts:
 - first draft early 2008.



Establishment of Watch, Warning and Incident Response (WWIR) Capabilities

- Assistance to Developing Countries related to Establishment of Watch, Warning and Incident Response (WWIR) Capabilities
- CSIRT Primer and Survey
- CSIRT Toolkit
- Inventory of Watch, Warning and Incident Response Capabilities by Region
- Standard Reporting Format for Fraudulent Online Activities

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



- 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



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 \(APCFRT\) 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

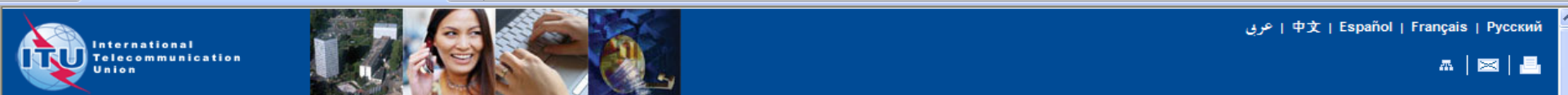
[More ITU-D resources]

Publications

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

Countering Spam and Related Threats

- Survey on Anti-Spam Legislation Worldwide
- Botnet Mitigation Toolkit for Developing Countries
 - Pilot Projects for Implementation of Toolkit (Malaysia)
- Joint Activities for StopSpamAlliance.org
- Study on Economics of Spam (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
 - <http://www.itu.int/ITU-D/cyb/cybersecurity/spam.html>



Home : [ITU-D : ICT Applications and Cybersecurity Division](#) : [Cybersecurity](#)

[Back to CYB](#)

[Home](#) | [ITU Sectors](#) | [Newsroom](#) | [Events](#) | [Publications](#) | [About Us](#)

- CYB Activities**
- [Cybersecurity](#)
- [E-Strategies](#)
- [ICT Applications](#)
- [Internet and IP Networks](#)
- [Telecentres](#)

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.

Newslog

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

[\[Browse CYB News Feeds\]](#)

- General Information**
- [Events](#)
- [Newslog](#)
- [Publications](#)
- [Contact CYB](#)
- [ITU-D Study Groups](#)
- [ITU-D Main Site](#)

Related Resources



Anti Spam Video From [antispam.br](#)



GOVCERT.NL's Botnet Movie



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 \(Antalya, 2006\)](#)
- [ITU WTDC Resolution 41: Mechanisms for enhancing cooperation on cybersecurity, including combating spam](#)
- [ITU WTSa Resolution 50: Cybersecurity \(Florianpolis, 2004\)](#)
- [ITU WTSa Resolution 51: Combating spam \(Florianpolis, 2004\)](#)
- [ITU WTSa Resolution 52: Countering spam by technical means \(Florianpolis, 2004\)](#)



Case Study: Botnets

- Botnets (also called zombie armies or drone armies) are networks of compromised computers infected with viruses or malware to turn them into “zombies” or “robots” — without the owners’ knowledge.
- 2007 generation botnets such as Zhelatin (Storm Worm) are particularly aggressive using advanced techniques such as **fast-flux networks** and **striking back with denial of service (DDOS) attacks** against security researchers or vendors trying to mitigate botnet
 - *“Fast-flux service networks are a network of compromised computer systems with public DNS records that are constantly changing, in some cases every few minutes. These constantly changing architectures make it much more difficult to track down criminal activities and shut down their operations.”*
 - Honeynet Project & Research Alliance





ITU Botnet Mitigation Toolkit

- ITU is developing a *Botnet Mitigation Toolkit* to help deal with the growing problem of botnets.
- Multi-stakeholder international cooperation and outreach
 - Phase 1 (2007): Downloadable toolkit/guidelines for ITU Member States
 - Phase 2 (2008/2009): Targeted national/regional pilot initiatives
 - Malaysia (MCMC)
- www.itu.int/ITU-D/cyb/cybersecurity/projects/botnet.html



Bridging the Security-Related Standardization Gap between Developing and Developed Countries (Plenipotentiary Resolution 123)

- Joint ITU-D/ITU-T Promotion of ITU-T Study Group 17 Activities
 - Joint ITU-T/ITU-D events
- Increased Deployment and Awareness in Developing Countries of ITU-T Security-Related Standards
- References
 - www.itu.int/ITU-D/cyb/cybersecurity/standards.html



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

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

Bridging the Security-Related Standardization Gap

ITU-T Study Group 17 is the lead study group for telecommunication security activities. ITU-T Study Group 17 produces materials that can be of interest and use to developing countries when identifying practical security solutions, an example of this is the newly revised [ICT Security Standards Roadmap](#). This roadmap captures network-related security work of not only ITU-T but also of ISO/IEC, IETF and consortia groups as part of their out-reach activities.

Joint ITU-T/ITU-D activities are currently undertaken to increase deployment and awareness in developing countries of ITU-T security-related standards. Information about existing ITU-T security standards are distributed widely to ITU Member States at ITU events worldwide to ensure that a larger number of participants from developing countries are involved in ITU's security standards development.

ITU Resolution 123 (Rev. Antalya, 2006) relates specifically to "Bridging the standardization gap between developing and developed countries". Links to some related activities and resources can be found below.

ITU-T Cybersecurity Activities

ITU-T Study Group 17 (in cooperation with other Study Groups and Working Parties) produces additional materials useful for developing countries including, for example:

- [ITU-T telecommunication security website](#)
- A Security Compendium including a "[Catalogue of approved ITU-T Recommendations related to telecommunication security](#)" and an "[Extract of ITU-T approved security definitions.](#)"
- Summaries of all Study Group 17 Recommendations under development or revision. (The [latest draft summaries.](#))
- [Document summarizing ITU-T security-related activities](#)
- [ITU-T Recommendation E.408: Telecommunication networks security requirements](#)
- [ITU-T Recommendation E.409: Incident organization and security incident handling: Guidelines for telecommunication organizations](#)

Background Resources for Security Standards

- The [ICT Security Standards Roadmap](#):
 - Part 1: [ICT Standards Development Organizations and Their Work](#)
 - Part 2: [Approved ICT Security Standards](#)
 - Part 3: [Security standards under development](#)

Search

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



Information Sharing through Enhancing the ITU Cybersecurity Gateway

- Establishment of an ITU Cybersecurity/CIIP Directory
- Establishment of an ITU Cybersecurity/CIIP Contact Database
- Establishment of Annual Who's Who in Cybersecurity/CIIP Publication
- Establishment of an Annual ITU Cybersecurity Publication
- ITU Cybersecurity Fellowship Programme for Developing Countries
- Enhancement of the ITU Cybersecurity Gateway
- References
 - <http://www.itu.int/cybersecurity/gateway/>

Regional Workshops on Frameworks for Cybersecurity/CIIP

- Hanoi, Vietnam
 - 28-31 August 2007
- Buenos Aires, Argentina
 - 16-18 Oct 2007
- Praia, Cape Verde (for West Africa)
 - 27-29 November 2007

- 2008 events planned
 - February 2008: Qatar/Oman (TBC)
 - End May 2008: Indonesia (TBC)
 - 7-9 October 2008: Sofia, Bulgaria (TBC)
 - Tunisia (TBC)
 - Africa

More Information

- ITU-D ICT Applications and Cybersecurity Division
 - www.itu.int/itu-d/cyb/
- ITU National Cybersecurity/CIIP Self-Assessment Toolkit
 - www.itu.int/ITU-D/cyb/cybersecurity/projects/readiness.html
- Regional Workshop on Frameworks for Cybersecurity and Critical Information Infrastructure Protection
 - www.itu.int/ITU-D/cyb/events/
- Botnet Mitigation Toolkit
 - <http://www.itu.int/ITU-D/cyb/cybersecurity/projects/botnet.html>
- Cybersecurity Publications
 - www.itu.int/ITU-D/cyb/publications/



International Telecommunication Union

Helping the World Communicate