ITU-D Cybersecurity Initiatives

ITU-T SG 17 Presentation
Geneva, Switzerland

24 September 2007

Robert Shaw <robert.shaw@itu.int>
Head, ICT Applications and Cybersecurity Division
Telecommunication Development Sector
International Telecommunication Union

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;

- In parallel with national consideration, move to international political agenda;

- Necessity to engage with many actors...

Many Relevant Actors in International Cybersecurity/CIIP Ecosystem

ITU 2007
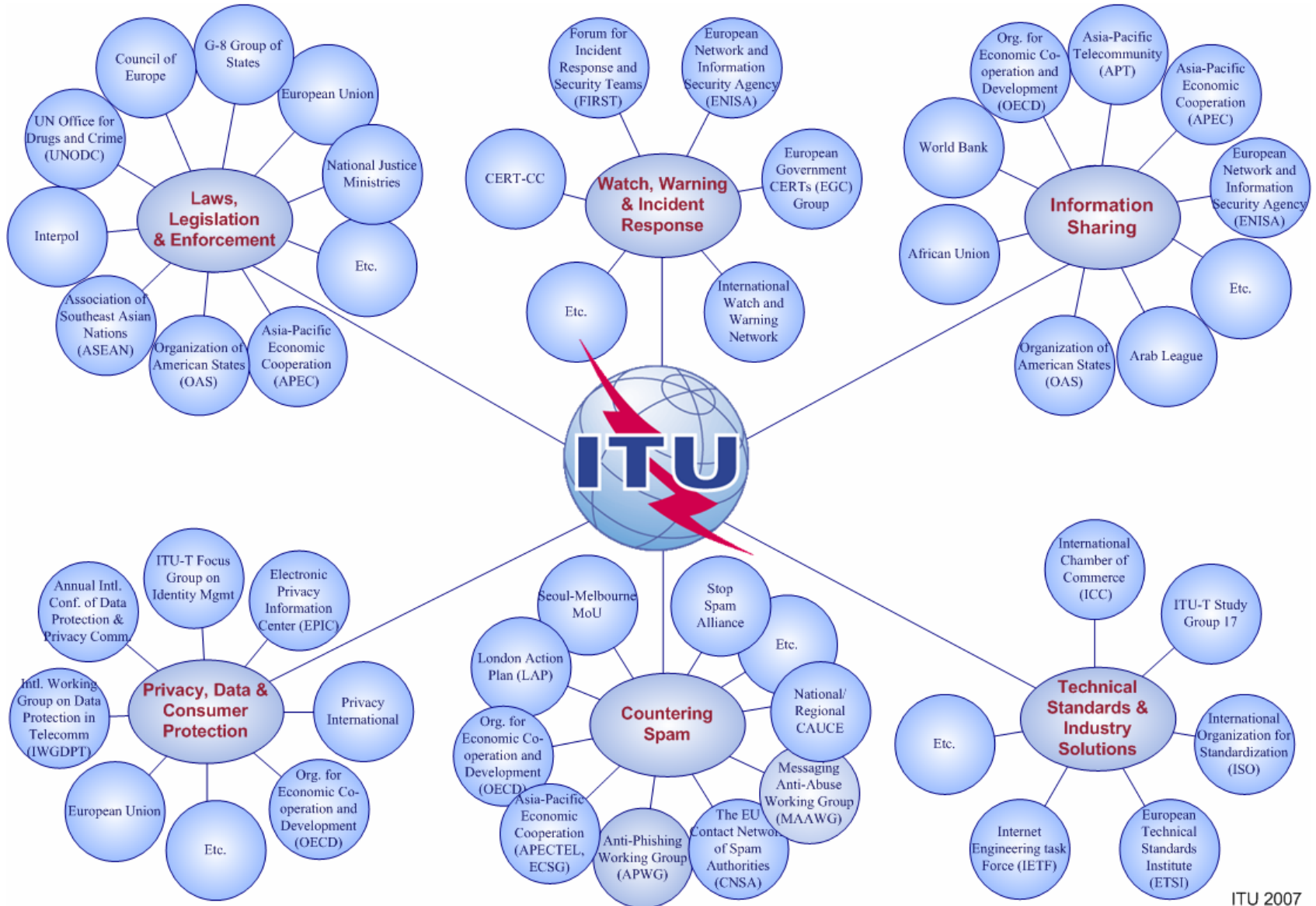
ITU Cybersecurity Work Programme to Assist Developing Countries

- Most countries have not formulated or implemented a national strategy for cybersecurity and Critical Information Infrastructure Protection (CIIP)
- Work Programme scopes a set of high level assistance activities
- Under these high level assistance activities, contains set of detailed initiatives planned in the 2007-2009 period by the ITU Development Sector's ICT Applications and Cybersecurity Division
- Extensive synergies with ITU-D Question 22/1: Securing information and communication networks: Best practices for developing a culture of cybersecurity
- Used to develop detailed operational plan for 2008-2009
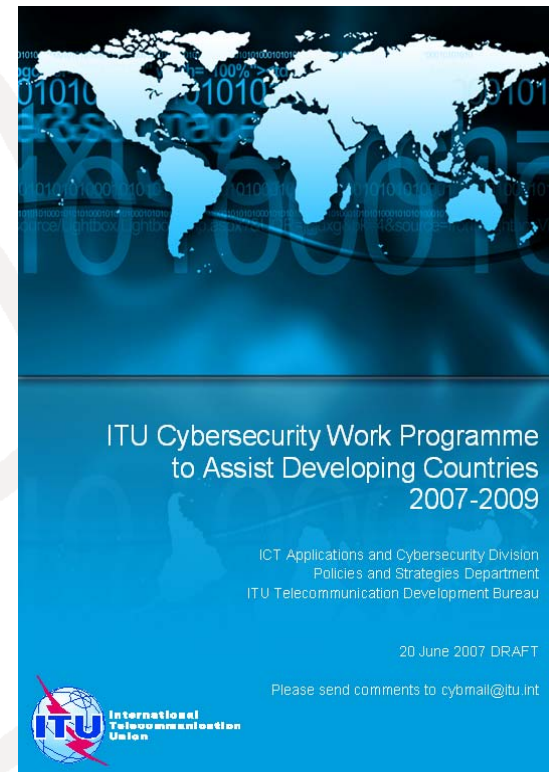
www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-cybersecurity-work-programme-developing-countries.pdf

ITU Cybersecurity Work Programme
to Assist Developing Countries
2007-2009

ICT Applications and Cybersecurity Division
Policies and Strategies Department
ITU Telecommunication Development Bureau

20 June 2007 DRAFT

Please send comments to cybmail@itu.int

High Level Elements

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

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

- 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

Google   Go   Bookmarks   8 blocked   Check   AutoLink   AutoFill   Send to   Settings

ITU-D ICT Applications and Cybersecurity (CYB) - Cyb...   Page   Tools

International Telecommunication Union

عربي | 中文 | Español | Français | Русский

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

Search   **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

Cybersecurity

Enhancing security and building confidence in the use of ICT applications is one of six priority domains for Programme 3 of the Doha Action Plan adopted at the 2006 World Telecommunication Development Conference. Links to ITU-D cybersecurity-related activities are below.

Highlights

- Work Programme Activities & Events
- ITU-D Study Group Activities
- Toolkits
- Background Resources
- Related Material

ITU-D Cybersecurity Web Pages

- National Strategies
- Legislation & Enforcement
- Warning & Incident Response
- Standards & Security
- Spam & Related Threats

Work Programme Activities and Related Events

ITU Cybersecurity Work Programme to Assist Developing Countries

- July 2007 Draft: ITU Cybersecurity Work Programme to Assist Developing Countries (2007-2009)

Events

- 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 Activities

Newslog

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

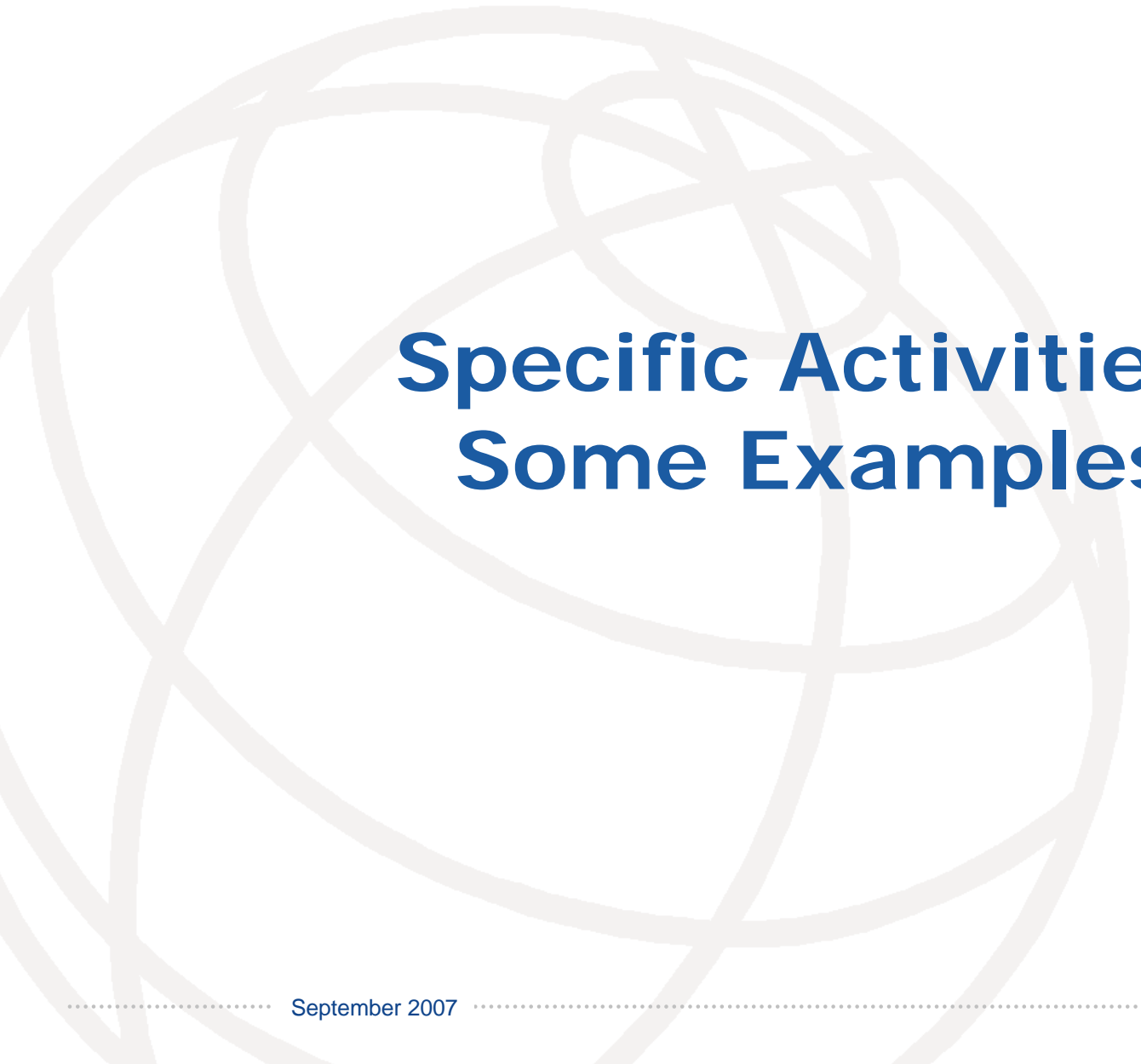[Browse CYB News Feeds]

Resources

ITU Cybersecurity Gateway

The ICT Eye

[More ITU-D resources]

Partnerships

StopSpamAlliance.org

Internet   100%

Specific Activities: Some Examples

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

- Identification of Best Practices in the Establishment of National Frameworks for Cybersecurity and CIIP
- Regional Workshops on Frameworks for Cybersecurity and CIIP
- National Cybersecurity/CIIP Readiness Self-Assessment Toolkit
- Online Cybersecurity 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/strategies.html
  - http://www.itu.int/ITU-D/cyb/events/
  - http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-cybersecurity-self-assessment-toolkit.pdf

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

EN

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

Google

Google | G- | Go | Bookmarks | 8 blocked | Check | AutoLink | AutoFill | Send to | Settings

ITU-D ICT Applications and Cybersecurity (CYB)

Page | Tools

International Telecommunication Union

عربي | 中文 | Español | Français | Русский

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

Visitor locations

ClustrMaps
Click to see

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

Establishment of Appropriate Cybercrime Legislation and Enforcement Mechanisms

- Regional Capacity Building Activities on Cybercrime Legislation and Enforcement
- Publication: Understanding Cybercrime: A Guide for Developing Countries (end 2007)
- Toolkit for Cybercrime Legislation for Developing Countries
- Cybersecurity Module in the ITU/InfoDev ICT Regulation Toolkit

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

International Telecommunication Union

عربي | 中文 | Español | Français | Русский

Search

Back to CYB

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 cybercrime 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**

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

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

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

- Assistance to Developing Countries related to Establishment of Watch, Warning and Incident Response (WWIR) Capabilities

- 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

ITU
International Telecommunication Union

عربي | 中文 | Español | Français | Русский

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

Visitor locations

ClustrMaps™
Click to see

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

Done   Internet   100%

Countering Spam and Related Threats

- Survey on Anti-Spam Legislation Worldwide
- Botnet Mitigation Toolkit for Developing Countries
- Pilot Projects for Implementation of Botnet Mitigation Toolkit in ITU Member States (Malaysia, India)
- 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
  - ➢ http://www.itu.int/ITU-D/cyb/cybersecurity/projects/botnet.html

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

EN

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

Google

Google | G- | Go | Bookmarks | 8 blocked | Check | AutoLink | AutoFill | Send to | Settings

ITU-D ICT Applications and Cybersecurity (CYB)

Page | Tools

International
Telecommunication
Union

عربي | 中文 | Español | Français | Русский

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

| **Back to CYB** | | **Home** | **ITU Sectors** | **Newsroom** | **Events** | **Publications** | **About Us** |

Search

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

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)

ITU WTDC Resolution 41: Mechanisms for enhancing cooperation on cybersecurity, including combating spam

ITU WTSA Resolution 50: Cybersecurity (Florianopolis, 2004)

ITU WTSA Resolution 51: Combating spam (Florianopolis, 2004)

ITU WTSA Resolution 52: Countering spam by technical means (Florianopolis, 2004)

Newslog

19 September 2007: ENISA / CERT/CC Workshop on Mitigation of Massive Cyberattacks

ITU News: Cybersecurity Watch September Edition

[Browse CYB News Feeds]

Related Resources

MAKE MILLIONS WORKING AT HOME
Tips and Tools at OnGuardOnline.gov

Anti Spam Video From antispam.br

NAVEGAR É PRECISO

GOVCERT.NL's Botnet Movie

Bridging the Security-Related Standardization Gap between Developing and Developed Countries (Plenipot 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

Regional Workshops on Frameworks for Cybersecurity/CIIP

- Hanoi, Vietnam
  - 28-31 August 2007
- Buenois Aires, Argentina
  - 16-18 Oct 2007
- Praia, Cape Verde (for West Africa)
  - 27-29 November 2007
- Egypt
  - 6-8 May 2008 (with Telecom Africa)
- Thailand
  - September 2008 (with Telecom Asia?)
- Caribbean, Africa, Bulgaria?
  - 2008

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

EN

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

Google

Go

Bookmarks ▾

8 blocked

Check ▾

AutoLink ▾

AutoFill

Send to ▾

Settings ▾

ITU-D ICT Applications and Cybersecurity (CYB)

Page ▾   Tools ▾

International Telecommunication Union

عربى | 中文 | Español | Français | Русский

Search

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

Home   ITU Sectors   Newsroom   Events   Publications   About Us

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

Newslog

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

[Browse CYB News Feeds]
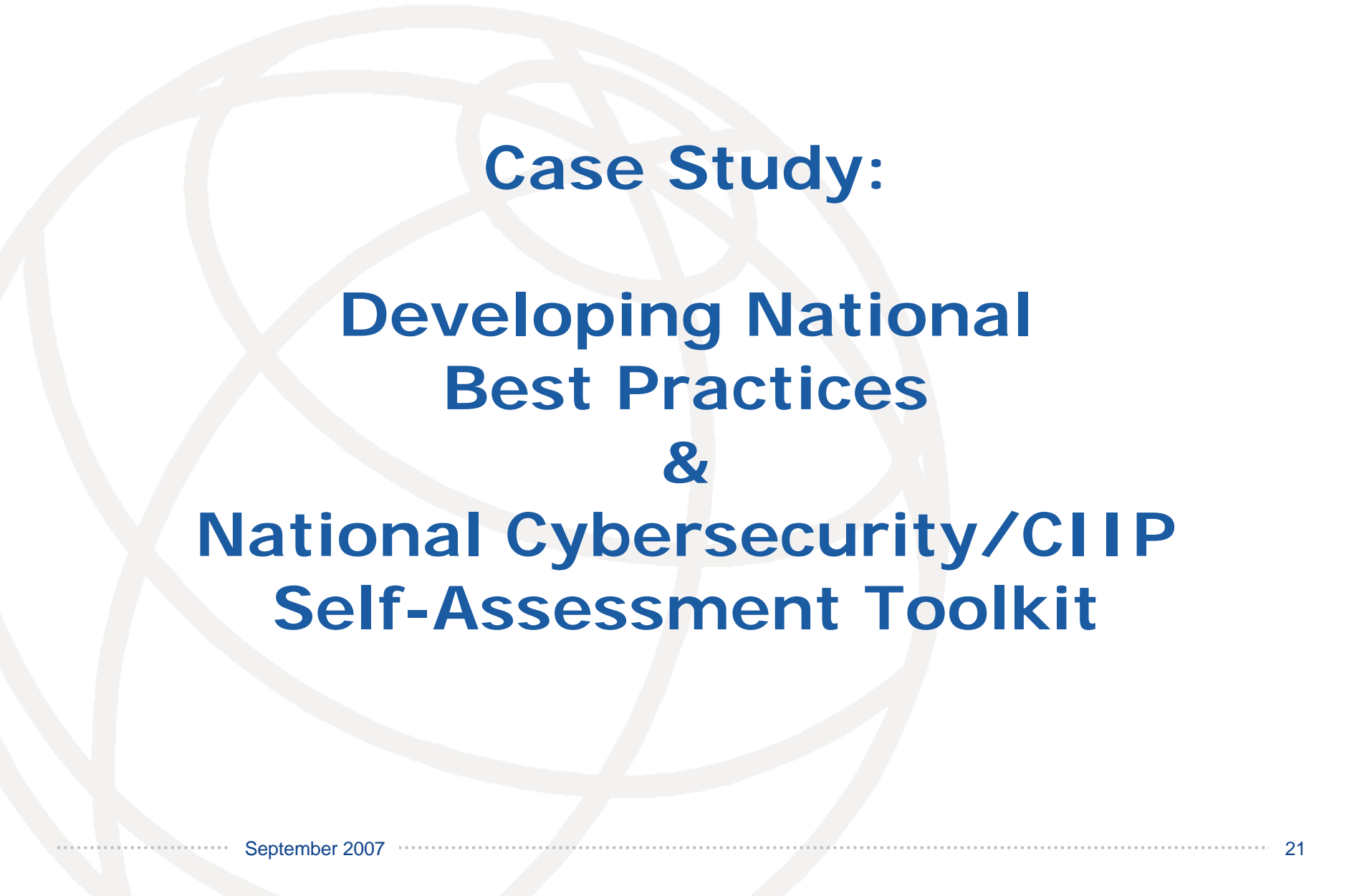
Resources

ITU Cybersecurity Gateway

The ICT Eye

[More ITU-D resources]

Publications

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

Internet   100%

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
  - ➢ Integration with ICT Eye?
  - ➢ Integration with Microsoft Virtual Earth or Google Earth

- References
  - ➢ http://www.itu.int/cybersecurity/gateway/

Case Study:

Developing National Best Practices & National Cybersecurity/CIIP Self-Assessment Toolkit

ITU-D Study Question 22/1

- Q.22/1: Study Question adopted at World Telecommunication Development Conference (WTDC): Securing information and communication networks: best practices for developing a culture of cybersecurity

- Calls for ITU Member States and Sector Members to create a report on best practices in the field of cybersecurity

- Four-year study cycle

- Pointer to Q.22/1 activities can be found at www.itu.int/ITU-D/cyb/cybersecurity/

ITU-D Q.22/1: Purpose

- To survey, catalogue, describe and raise awareness of:
  - ➤ The principal issues faced by national policy makers in building a culture of cybersecurity
  - ➤ The principal sources of information and assistance related to building a culture of cybersecurity
  - ➤ Successful best practices employed by national policy-makers to organize for cybersecurity
  - ➤ The unique challenges faced by developing countries

- To examine best practices for watch, warning, and incident response and recovery capabilities

Q22.1 Draft Report (Sept 2007)

- 5 key elements to a good national cybersecurity programme:
  - ➤ A national strategy
  - ➤ A sound legal foundation to deter cybercrime
  - ➤ A national incident management capability
  - ➤ Collaboration between Government and Industry
  - ➤ A national awareness of the importance of a culture of cybersecurity
- Current draft at
  - ➤ www.itu.int/md/D06-SG01-C-0088/en

Self–Assessment Toolkit

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

Self-Assessment Toolkit cont'd

- Looks at organizational issues for each element of the Framework
  - *The people*
  - *The institutions*
  - *The relationships*
  - *The policies*
  - *The procedures*
- Toolkit now in draft form
  - www.itu.int/md/D06-SG01-C-0122/en

Self-Assessment Toolkit cont'd: Deterring Cybercrime 'Tab'

- Necessary elements of substantive, procedural and mutual assistance law
- Allows national authorities to review their domestic situation related to the goals and actions identified in:
  - UN General Assembly Resolution 55/63 (2000)
    - http://www.un.org/Depts/dhl/resguide/gares1.htm
  - Council of Europe's Convention on Cybercrime (2001)
    - http://www.coe.int/T/E/Com/Files/Themes/Cybercrime/

- Survey adapted from work in APEC-TEL Working Group
  - http://www.apectelwg.org/e-securityTG/Resources.htm.
  - See www.itu.int/ITU-D/cyb/cybersecurity/legislation.html

Self-Assessment Toolkit cont'd

- National Pilot Tests
  - ➢Vietnam (2007)
  - ➢Argentina (TBC 2007)
  - ➢Ghana (2007)

- To express interest in participating in pilot tests, contact cybmail@itu.int

Case Study:
ITU Botnet Mitigation Toolkit

Botnets – An Overview

- **What is a Botnet?**
  - ➢ A collection of infected and compromised computing devices harnessed together and remotely controlled for malicious purposes

- **How powerful is a Botnet?**
  - ➢ Like supercomputers created through distributed computing systems
    - e.g., BOINC: used for SETI@Home, Atomic Physics
    - People agree to donate spare computing resources
  - ➢ Botnets: a special case of distributed computing
    - Without consent of computer owner (a zombie)
    - Hijacking of computing resources

Botnets – An Overview cont'd

- Botnets are a worldwide menace, widely used by spammers and cyber criminals
- Use of botnets for cybercrime has increased and become more refined since 2002-3 when first mass mailer worms such as Sobig and Sober were released

Latest Generation

- 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

The Botnet Ecosystem

- Virus Writers, Botherders, Clients
  - ➤ Virus writer writes malware, infects computers to create botnet
  - ➤ Botherder operates the botnet "command and control" (C&C)
  - ➤ Clients hire botnets to distribute spam, launch Distributed Denial of Service (DDoS) attacks, to conduct identity theft
- Highly developed underground channels of communication
  - ➤ "Secret" forums/chat rooms that shift location
  - ➤ Access on a need to know basis, new entrants may need to be vouched for by existing participant

The Botnet Ecosystem cont'd

- Botherders now offer "service level agreements" to clients
  - ➤ Guaranteed replacement of botnet in case anti-virus researchers release fix for malware or botnet is taken down
- Organized crime involved in all stages of ecosystem
  - ➤ Employ virus writers to create malware
  - ➤ Carry out spam campaigns, espionage, ID theft, cyber-attacks
 - ➤ Laundering of money stolen from victims

Evolution of Botnets

- C&C centers harder to trace
  - ➤ Originally hosted on public IRC channels
  - ➤ Now encrypted, access restricted C&C software
- C&C centers may be hosted on botnets
  - ➤ Increased redundancy
  - ➤ Makes takedown harder
- New "headless" single use botnets
  - ➤ No centralized control or C&C required
    - new generation of P2P botnets
  - ➤ Instructions embedded into malware
  - ➤ New malware and botnet created for a new task
  - ➤ Cannot stop botnet by taking down its C&C

Evolution of Malware

- Self-propagating: infected hosts infect other hosts
  - ➢ Infection vectors include email, P2P networks, open shared network folders, Skype, visiting infected website
  - ➢ Newer malware spreads faster than older generations
- Spread resembles global pandemic (SARS, Bird Flu)
  - ➢ Can similar threat models/mitigation mechanism theories be applied?
- Analysis, Detection and Removal more difficult
  - ➢ Self-destruct mechanisms to destroy data if malware removed
  - ➢ "Droppers" malware download more payload onto compromised host
  - ➢ Encryption and debuggers / Virtual Machine (VM) traps to prevent forensic analysis
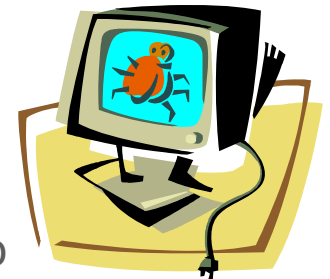
What can you do with a Botnet?

- Send spam
  - ➢ Most visible use of botnets
  - ➢ Botnets can host entire spam campaign
    - Including DNS servers, website hosting, spam sending
    - Content can change location from PC to PC, country to country, in minutes
  - ➢ "Take" from a spam run can be reused
    - 419 scam artists now buying lists of compromised accounts from botherders, using these to spam
  - ➢ But spam is just the tip of the iceberg

What else can you do with a Botnet?

- Attack a country's Internet infrastructure
  - ➢ Estonia DDoS attacks
- Extortion/Blackmail
  - ➢ Threaten to DDoS/cripple e-commerce websites
- Identity theft and Industrial Espionage
  - ➢ Steal credit cards, passwords, etc. from infected PCs
  - ➢ Use computing power of a botnet to break into secured networks and steal data, credit cards
- Stock "Pump and Dump" scams
  - ➢ Use spam from botnet PCs to advertise stock
  - ➢ Trade in this stock using online share trading accounts from infected PCs, artificially boost prices

ITU Botnet Mitigation Project inspired by Australian Internet Security Initiative (AISI)

- Australian Communications and Media Authority (ACMA) partnership with 25 Australian ISPs
  - ➤ ACMA collects data on IPs emitting malware
    - Identifies IPs operated by participating Australian ISPs
    - Notifies ISP responsible for affected IPs
  - ➤ ISPs undertake to mitigate malware activity from infected IPs on their networks
    - Notify infected customers
    - Change security and filtering policies as necessary
- AISI project working internationally to fight botnets and has agreed to extend AISI to other ITU Member States

ITU Botnet Mitigation Package

- Identify nodal coordination agency for a nationwide botnet mitigation strategy
  - ➢ Multi-stakeholder, Multi-pronged Approach (like OECD spam toolkit)
  - ➢ Public-Private Partnership
  - ➢ Make best possible use of existing initiatives and structures
- Infrastructure for botnet scanning, measurement and mitigation
  - ➢ Capacity building on tools and techniques to track botnets
  - ➢ Identification of trusted interlocuters (e.g., international security and AV research community, CERT teams) for incident reporting

ITU Botnet Mitigation Package

- Detection and takedown of botnet hosts and related infrastructure
  - ➢ Infected PCs (automate as far as possible), C&C hosts, domains registered for botnet, payment gateways used by botnets, etc
- Build awareness of security best practices for ISPs, e-commerce sites
- Promote general Internet safety through end-user awareness programmes, engagement of civil society for assistance and grassroots penetration

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 pilot initiatives
    - Malaysia (MCMC), India (CERT-IN)
  - ➤ Cooperation with other partners?
    - LAP, APEC-TEL, OECD, MAAWG, APWG, Interpol, ENISA, CERT/CC?

More Information

- ITU-D ICT Applications and Cybersecurity Division
  - ➤ www.itu.int/itu-d/cyb/
- ITU National Cybersecurity/CIIP Self-Assessment Toolkit: Background & Approach
  - ➤ www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-cybersecurity-national-self-assessment-toolkit.pdf
- ITU Botnet Project Website
  - ➤ www.itu.int/ITU-D/cyb/cybersecurity/projects/botnet.html
- ITU Botnet Mitigation Toolkit Overview
  - ➤ www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-botnet-mitigation-toolkit.pdf
- Regional Workshops on Frameworks for Cybersecurity and Critical Information Infrastructure Protection
  - ➤ www.itu.int/ITU-D/cyb/events/

International Telecommunication Union

Helping the World Communicate