Cybersecurity for ALL

ITU's Work for a Safer World

International Telecommunication Union

Committed to connecting the world

An Overview of ITU-D's Cybersecurity Activities & ITU Botnet Mitigation Project

Regional Seminar on Costs and Tariffs
Regional Group for Asia and Oceania (SG3RG-AO)

4-5 March 2009

Suresh Ramasubramanian
Consultant for the
ITU Telecommunication Development Bureau
ICT Applications and Cybersecurity Division <cybmail@itu.int>

For more information on **ITU Cybersecurity Activities**
see: www.itu.int/cybersecurity/

International Telecommunication Union

Committed to connecting the world

ITU: A Forum for International Cooperation in Cybersecurity

- ITU Secretary-General has identified cybersecurity as a top priority
  - **ITU Global Cybersecurity Agenda (GCA)**: *A Global Strategy for Action*
- ITU Membership is calling for a greater role to be played by ITU in matters relating to cybersecurity through various Resolutions, Decisions, Programmes and Recommendations
  - **ITU Strategic Goal Four**: "*Developing tools, based on contributions from the membership, to promote end-user confidence, and to safeguard the efficiency, security, integrity and interoperability of networks*"
  - **ITU Plenipotentiary Conference Resolution 130**: "*Strengthening the role of ITU in building confidence and security in the use of information and communication technologies*" (Antalya, 2006)

International Telecommunication Union

Committed to connecting the world

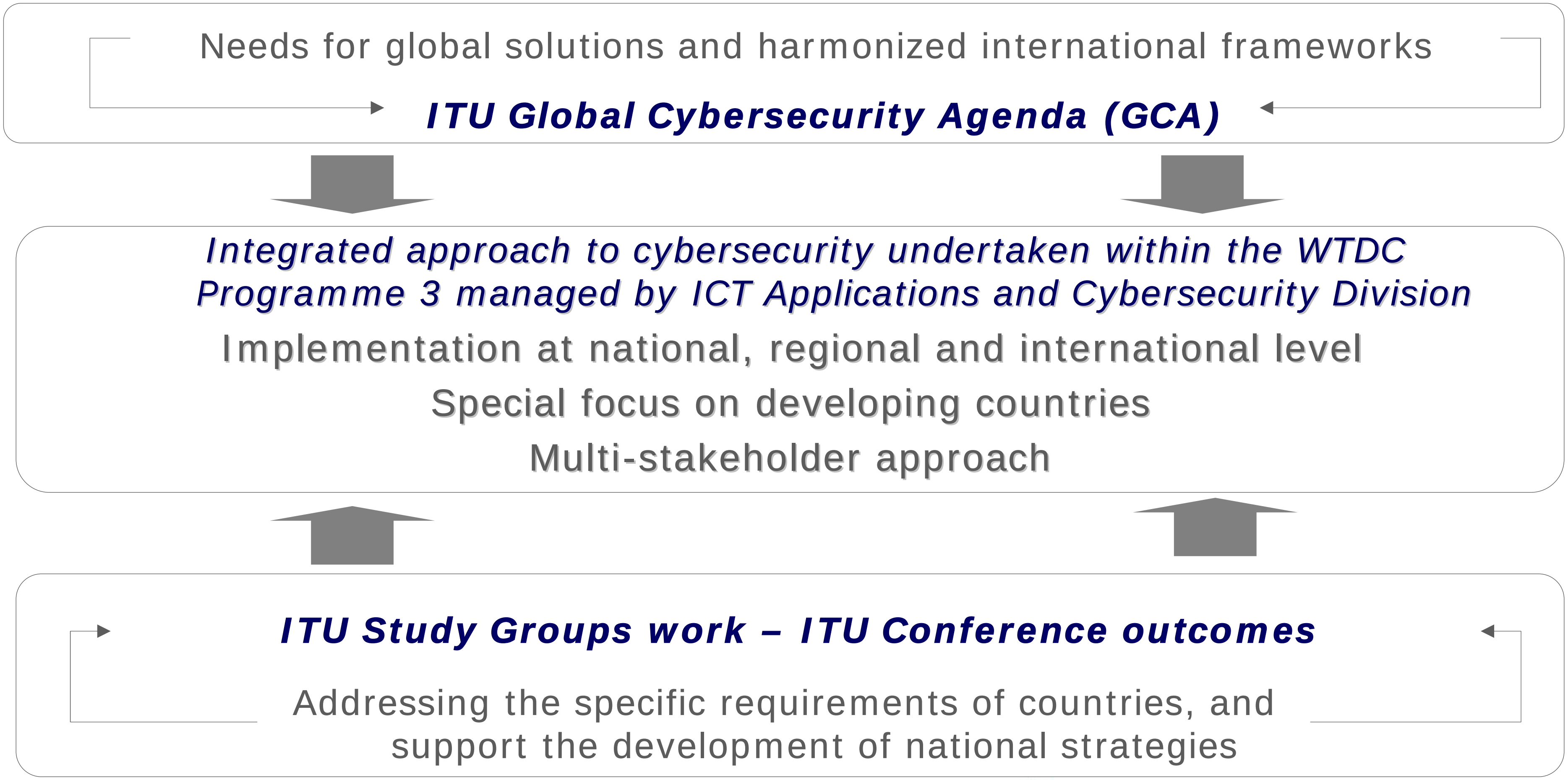
ITU's Role as WSIS C5 Facilitator

- At the World Summit on the Information Society (WSIS), world leaders and governments **entrusted ITU** to take the leading role in coordinating international efforts on cybersecurity, as the sole facilitator for Action Line C5: **"Building confidence and security in the use of ICTs"**
- ITU provides a global perspective and the expertise needed, **promoting cybersecurity** through a range of activities related to **standardization, radiocommunication** and **technical assistance to developing countries**, tailored to countries' needs.

Third WSIS C5 Facilitation Meeting
was held in Geneva, 22-23 May 2008
www.itu.int/osg/csd/cybersecurity/WSIS/3rdMeeting.html

Forth WSIS C5 Facilitation Meeting
will take place in Geneva in May 2009

Cybersecurity in ICT Development



Needs for global solutions and harmonized international frameworks

ITU Global Cybersecurity Agenda (GCA)

Integrated approach to cybersecurity undertaken within the WTDC Programme 3 managed by ICT Applications and Cybersecurity Division

Implementation at national, regional and international level

Special focus on developing countries

Multi-stakeholder approach

ITU Study Groups work – ITU Conference outcomes

Addressing the specific requirements of countries, and support the development of national strategies

International Telecommunication Union

Committed to connecting the world

ITU Development Sector (ITU-D) Work in Cybersecurity

Background and Mandate

- From ITU Plenipotentiary Conference (Antalya, 2006):
  - Resolution 130: Strengthening the role of ITU in building confidence and security in the use of information and communication technologies
- From World Telecommunication Development Conference (Doha, 2006):
  - ITU-D Study Group 1 Question 22/1
  - Resolution 45
  - Cybersecurity part of *Programme 3* managed by *ITU-D ICT Applications and Cybersecurity Division*

Cybersecurity in ITU-D

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

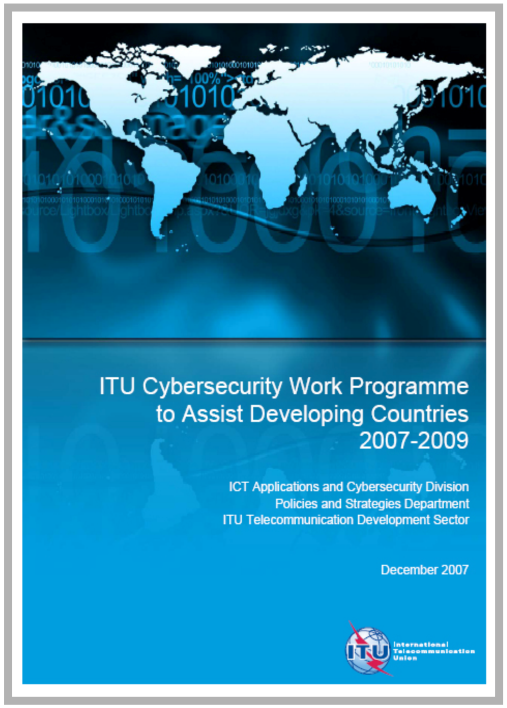
International Telecommunication Union

Committed to connecting the world

ITU Cybersecurity Work Programme to Assist Developing Countries

- Most countries have not yet formulated or implemented national strategies for cybersecurity and/or Critical Information Infrastructure Protection (CIIP)
- ITU-D Work Programme scopes a set of high level assistance activities
- Also scopes detailed activities and initiatives planned to be implemented by the *ITU Development Sector's ICT Applications and Cybersecurity Division* together with Member States, private and public sector partners, and other regional and international organizations
- More details about the *ITU-D Cybersecurity Work Programme to Assist Developing Countries* can be found at:

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 Sector

December 2007

International
Telecommunication
Union

Committed to connecting the world

ITU-D Areas of Activities

- Assistance related to Establishment of National Strategies and Capabilities for Cybersecurity and Critical Information Infrastructure Protection (CIIP)
  - ITU National Cybersecurity/CIIP Self-Assessment Tool
- 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
- Child Online Protection Activities
- 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

International Telecommunication Union

Committed to connecting the world

Examples of Some ITU-D Efforts to Support the Development of Cybersecurity Capacity

International Telecommunication Union

Committed to connecting the world

National Strategies/Capabilities for Cybersecurity and CIIP

- Reference material and training resources
- Assistance in the establishment of National Strategies for Cybersecurity and CIIP
- Some Tools:
  - ITU National Cybersecurity/CIIP Readiness Self-Assessment Tool
  - ITU Botnet Mitigation Toolkit
  - ITU Study on the Financial Aspects of Network Security: Malware and Spam
- ITU Regional Cybersecurity Forums
  - 2007: Vietnam, Argentina, Cape Verde
  - 2008: Qatar, Australia, Zambia, Bulgaria
  - 2009: events planned
- 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/

International Telecommunication Union

Committed to connecting the world

Establishment of Cybercrime Legislation and Enforcement Mechanisms

- Regional capacity building activities on Cybercrime Legislation and Enforcement
- Understanding Cybercrime Publication:
  - To be published in the coming months
- ITU Toolkit for Cybercrime Legislation:
  - To be published in the coming months
- References:
  - www.itu.int/ITU-D/cyb/cybersecurity/legislation.html
  - www.itu.int/ITU-D/cyb/cybersecurity/projects/cyberlaw.html

Establishment of Watch, Warning and Incident Response Capabilities

- Assistance to Developing Countries in the Establishment of Watch, Warning and Incident Response (WWIR) Capabilities
  - Coordination and cooperation with key players (FIRST, etc.)
  - e.g. facilitate the establishment of a Pacific CERT (2009)
- Activities related to the establishment of Computer Security Incident Response Teams (CSIRTs)
  - CSIRT survey
  - CSIRT toolkit
  - Inventory of watch, warning and incident response capabilities by region
- References:
  - www.itu.int/ITU-D/cyb/cybersecurity/wwir.html

ITU Botnet Mitigation Project

An Overview

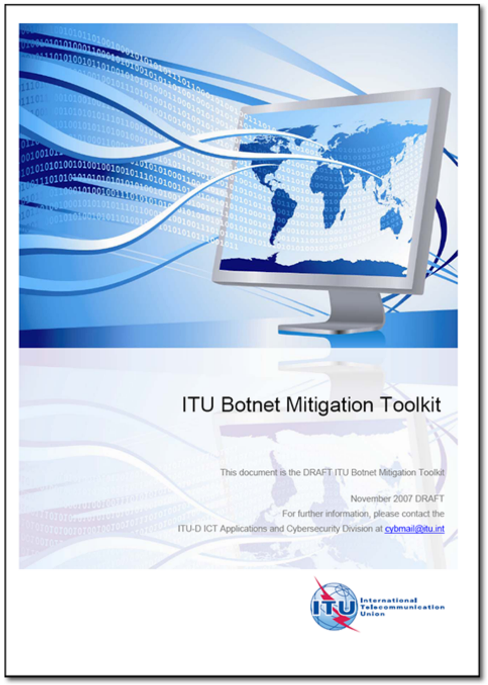
For more information on the
ITU Botnet Mitigation Project see project website at:
www.itu.int/ITU-D/cyb/cybersecurity/projects/botnet.html
or e-mail cybmail@itu.int

International Telecommunication Union

Committed to connecting the world

General Principles of The Toolkit

- This concept is based on several previous cybersecurity initiatives, not necessarily botnet focused.
- Multi-stakeholder, Multi-pronged initiatives required, No Silver Bullet ..
  - Yes, these are clichés, but they're still true.
  - Technical measures alone wont be enough, nor will laws.
- The toolkit is based on:
  - The context of a larger cybersecurity readiness strategy
  - Top down and bottom up public-private partnerships between government, industry, technical community, civil society
  - Optimum use of existing initiatives and structures



ITU Botnet Mitigation Toolkit

This document is the DRAFT ITU Botnet Mitigation Toolkit

November 2007 DRAFT

For further information, please contact the
ITU-D ICT Applications and Cybersecurity Division at cybmail@itu.int

International Telecommunication Union

International Telecommunication Union

Committed to connecting the world

Original Inspiration : Australian Internet Security Initiative (AISI)

- Australian Communications and Media Authority 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
    - Notify infected customers
    - Change security and filtering policies as necessary
- AISI project working internationally to fight botnets and has agreed to assist the ITU project and extend AISI to other ITU Member States

ITU Botnet Mitigation Package

- Identify coordination agency for a nationwide botnet mitigation strategy
  - Multi-stakeholder, Multi-pronged Approach (like OECD spam toolkit)
  - Public-Private Partnership
  - Coordination of local and global efforts
  - 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 interlocutors (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 guidelines and background paper available on the ITU website.
  - Phase 2 (2008/2009): Targeted national/regional assistance initiatives
    - First pilot in Malaysia – begins early 2009
  - Cooperation with other partners
    - LAP, APEC-TEL/OECD, Interpol, and other groups (MAAWG, APWG, FIRST, Shadowserver, Spamhaus..)

ITU International Telecommunication Union
Committed to connecting the world

Planned Malaysia Pilot - Overview

- Facilitated by the Malaysian Communications and Multimedia Commission (MCMC)
- A white paper on existing practical application of concepts advocated by the toolkit
  - Instances of application of the concepts and suggested best practices mentioned in the toolkit
  - Practices followed by policy, technical and civil society groups in Malaysia highlighted, results observed, feedback collected.
  - What worked? What didn’t work? What modifications were required to currently accepted best practices to make them work together?

International Telecommunication Union

Committed to connecting the world

AISI Malaysia Pilot

- Goal: Implement AISI in Malaysia
  - Source feeds from various sources
    - Anti-malware / antispam groups, CERTs, Honeypot networks …
    - Preferably in the RFC standardized IODEF format
  - Extend to (say) two ISPs as an initial pilot
    - ISPs agree and volunteer to receive these reports
      - And to mitigate abuse on their networks based on these reports
    - ISPs contribute and update their ASNs / IP address space that they wish to receive alerts for
  - Then implement at other ISPs over the course of the pilot and afterwards

ITU International Telecommunication Union

Committed to connecting the world

Workshops

- Policy and Technical Workshops
  - Policy workshops focused on government (regulators, law enforcement, judiciary) personnel
  - Technical workshops focused on "in the trenches" mitigation by ISPs and Industry
- Workshop material made available for future education initiatives
  - Translated into the UN official languages
  - Additionally, the MAAWG best practice documents are currently being translated into the official UN languages

Technical Workshops

- Workshop for ISPs / NSPs
  - Instructors from Cisco / NSP-SEC
  - Hosted at Universiti Sains Malaysia, Penang
- Workshop for banks & ecommerce sites
  - Facilitated by the Anti-Phishing Working Group (APWG)
  - Two workshops, one high level, for senior management and another with hands on operational content
  - Instructors from Wachovia Bank (TBC)

International Telecommunication Union

Committed to connecting the world

Policy Workshops

- A series of policy focused workshops
  - Focused on different government departments and their needs
    - Regulators, Law Enforcement Agencies, Prosecutors, Judiciary …
- Workshops and briefing sessions on the sidelines of an international conference on cybersecurity and botnets, to be hosted jointly by ITU and MCMC (TBC)

Feedback and Participation

- ITU welcomes comments on the Botnet Mitigation Toolkit and the pilot project
- ITU would also appreciate insights into similar field testing of best practices, especially in emerging economies, if available
- Offers of assistance (such as providing reporting feeds, workshop instructors or anything else) are welcome.
- Project email address : cybmail@itu.int

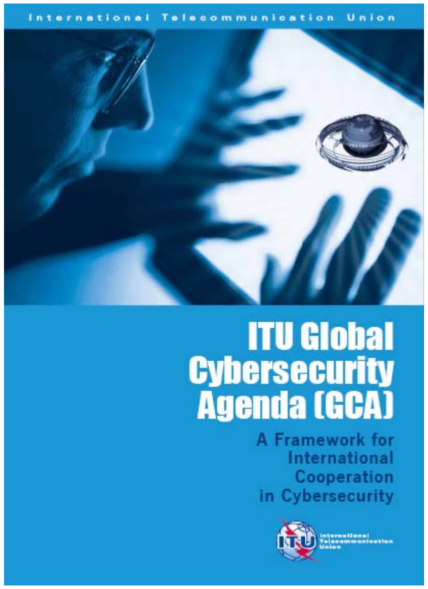
A Global Response:
ITU Global Cybersecurity Agenda (GCA)

A Global Response

The GCA aims to bridge existing initiatives and partners with the objective of proposing global strategies to address today’s challenges in the fight against cybercrime and to maintain cyber-peace.

ITU Global Cybersecurity Agenda (GCA)

- A framework for international multi-stakeholder cooperation in cybersecurity
- ITU Response to its role as sole Facilitator for WSIS Action Line C5
- World renowned Group of High Level Experts (HLEG) to develop global strategies
- Specific initiatives undertaken under GCA


International Telecommunication Union

ITU Global Cybersecurity Agenda (GCA)

A Framework for International Cooperation in Cybersecurity

International Telecommunication Union

International Telecommunication Union

Committed to connecting the world

Outcomes of the GCA

- The momentum generated by the GCA and the broad nature of this ITU initiative have resulted in interest from other stakeholders and opportunities for collaboration and cooperation.
- Specific initiatives are being undertaken under GCA umbrella, including:
  - IMPACT & GCA
  - Child Online Protection (COP) Initiative & GCA

International Telecommunication Union

Committed to connecting the world

IMPACT & GCA

- The Government of Malaysia offered to make available the infrastructure of the International Multilateral Partnership Against Cyber-Terrorism (IMPACT) as the physical home of the Global Cybersecurity Agenda(GCA).
- ITU is facilitating the implementation and establishment of cybersecurity capabilities making use of the services provided by IMPACT in the areas of:
  - Real-time analysis, aggregation and dissemination of global cyber-threat information;
  - Early warning system and emergency response to global cyber-threats; and
  - Training and skills development on the technical, legal and policy aspects of cybersecurity.

International Telecommunication Union

Committed to connecting the world

ITU Child Online Protection (COP) Initiative & GCA

An international collaborative network of multi-stakeholder and multi-sectoral partnerships for the development of a common framework for the protection of children online through:

- Education and Training
- Infrastructure and Technology
- Policies and Practices
- Awareness and Communication

International Telecommunication Union

Committed to connecting the world

Towards Global Cyberpeace…

The threats to global cybersecurity demand a global framework

"The magnitude of this issue calls for a coordinated global response to ensure that there are no safe havens for cybercriminals.

*ITU, through its **Global Cybersecurity Agenda** will act as a catalyst and facilitator for these partners to share experience and best practice, so as to step up efforts for a global response to cybercrime.*

In this way, working together, we can create a cyberspace that is somewhere safe for people to trade, learn and enjoy."

Dr Hamadoun I. Touré
ITU Secretary-General

International Telecommunication Union

Committed to connecting the world

More Information

- An Overview of ITU Activities in Cybersecurity
  - www.itu.int/cybersecurity/
- ITU Global Cybersecurity Agenda
  - www.itu.int/cybersecurity/gca/
- ITU-D ICT Applications and Cybersecurity Division
  - www.itu.int/ITU-D/cyb/
- ITU-D Cybersecurity Resources
  - www.itu.int/ITU-D/cyb/cybersecurity/
- Regional Cybersecurity Forums and Conferences
  - www.itu.int/ITU-D/cyb/events/
- ITU Child Online Protection (COP) Initiative
  - www.itu.int/cop/

Thank You!

For more information on
ITU's Cybersecurity Activities see:

www.itu.int/cybersecurity/

www.itu.int/ITU-D/cyb/
or e-mail cybmail@itu.int

International
Telecommunication
Union

Committed to connecting the world