Cybersecurity for ALL

An Overview of ITU’s Cybersecurity Activities

CTO meeting
25, 26 April 2013
Yaoundé
ITU International Cooperation on Cybersecurity

Jean-Jacques MASSIMA-LANDJJI,
ITU Representative for Central Africa and Madagascar

jean-jacques.massima@itu.int
Why International Cooperation?

Phenomena of Cybercrime

► The victim can be anywhere around the globe while the criminal is operating in elsewhere in far away

► The challenges are inherently international in scope and require international cooperation, investigative assistance, and common substantive and procedural provisions

Harmonization on legal framework

► Thus, it is important that countries harmonize their legal frameworks to combat cybercrime and facilitate international cooperation.
Legal Challenges to Fight Against Cybercrime

- Challenges in Drafting National Criminal Laws
  
  The main challenge for national criminal legal systems is the delay between the recognition of potential abuses of new technologies and necessary amendments to the national criminal law. This challenge remains as relevant and topical as ever as the speed of network innovation accelerates.

- Increasing Use of ICTs and the Need for New Investigative Instruments
  
  Recent developments in ICTs have not only resulted in new cybercrimes and new criminal methods, but also new methods of investigating cybercrime. Advances in ICTs have greatly expanded the abilities of law enforcement agencies. Conversely, offenders may use new tools to prevent identification and hamper investigation.
Global Framework for Cybersecurity

At the World Summit on the Information Society (WSIS) in 2005, ITU was entrusted by leaders of the international community to act as the facilitator for

WSIS Action Line C5:

“Building confidence and security in the use of ICTs”
ITU Global Cybersecurity Agenda

“Building confidence and security in the use of ICTs”

In 2007, ITU Secretary-General launched the Global Cybersecurity Agenda, an international framework for collaboration on Cybersecurity matters that addresses five main areas:

1. Legal Measures
2. Technical and Procedural Measures
3. Organizational Structure
4. Capacity Building
5. International Cooperation
Legal Measures

- **Summary of objective:**
  Harmonization of legal frameworks and the elaboration of strategies for cybercrime legislation globally applicable and interoperable with national/regional legislative measures

**Related activities/initiatives**

**Resources**
- ITU Cybercrime Legislation Resources
- ITU Toolkit for Cybercrime Legislation

**Publications**
- ITU Publication on Understanding Cybercrime: A Guide for Developing Countries

**Training and Events**
- Capacity building, training (training for judges, etc.)
- Regional workshops and events
Examples of Recent Initiatives

**ITU Toolkit for Cybercrime Legislation** aims to provide countries with sample legislative language and reference material that can assist in the establishment of harmonized cybercrime laws and procedural rules.

**ITU Publication on Understanding Cybercrime: A Guide for Developing Countries** provides a comprehensive overview of the most relevant topics linked to the legal aspect of cybersecurity and cybercrime.

www.itu.int/ITU-D/cyb/cybersecurity/legislation.html
**Technical and Procedural Measures**

**Summary of objective:** Development of strategies for the establishment of globally accepted security protocols, standards, minimum security criteria and accreditation schemes for hardware and software applications and systems.

**Related activities/initiatives**

**Security Activities**
- ITU Standardization Work
- ICT Security Standards Roadmap promoting collaboration
- ITU Radiocommunication security activities

**Study Groups**
- ITU-T Study Group 17
- ITU-T Study Group 2
Organizational Structures

- **Summary of objective:**
  Elaboration of global strategies for the creation of appropriate national and regional organizational structures and policies on cybercrime, watch, warning and incident response and universal identity systems.

**Related activities/initiatives**

**Partnerships**
- International Multilateral Partnership Against Cyber Threats (IMPACT) collaboration services
- Partnerships with other entities to deliver specific services to Member States

**Projects**
- Development of national computer incident response teams (CIRTs) and watch, warning and incident response related training
- Etc.

**Training/ Assistance**
- Capacity building and training
- Regional workshops and events
- Direct assistance to countries

ITU Secretary-General Dr Hamadoun Touré
Capacity Building

- Summary of objective:
  Development of global strategies to facilitate human and institutional capacity building across all relevant aspects of cybersecurity

Related activities/initiatives

**Toolkits and Resources**
- ITU National Cybersecurity/CIIP Self-Assessment Tool
- ITU Toolkit for Promoting a Culture of Cybersecurity
- ITU Botnet Mitigation Toolkit and pilot projects

**IMPACT Project**
- IMPACT Training and Skills Development Centre
- IMPACT Research Division

**Training and Events**
- Capacity building and training across all the pillars of the GCA
- Targeted workshops and events
Summary of objective:
Development of proposals to enhance international dialogue on issues that pertain to cybersecurity and enhance cooperation and coordination across all relevant activities.

Related activities/initiatives

Working Together
- ITU Secretary-General High Level Expert Group (HLEG) deliverables

Information Sharing
- ITU-IMPACT collaboration
- ITU Cybersecurity Gateway
- ITU’s Child Online Protection (COP) initiative

Conferences/Events
- World Telecommunication and Policy Forum WTPF 2009
- Regional cybersecurity forums
National Cybersecurity Agency: Examples

- **Canada**: Canadian Cyber Incident Response Centre (CCIRC) – Integrated within the Strategic Government Operations Centre (GOC)
- **Australia**: Australian Cybersecurity Policy and Co-ordination Committee (CSPC – Nov 2009), within the Attorney-General’s Government Dept
- **Malaysia**: “Cybersecurity Malaysia” – Mosti: Ministry of Science, Technology & Innovation, and includes the MyCERT & Training Centre
- **Singapore**: Cybersecurity Awareness Alliance & the IDA Security Masterplan (Sept 2009) - Singapore Infocomm Technology Security Authority - SITSA
- **South Korea**: Korea Internet and Security Agency (KISA – July 2009)
- **Cameroon, Congo, Gabon**: Agencies in charge of Cyber security installed.

.....Many nations are now also following similar National Strategies, using their National CIRTs as the focus & catalyst to develop National Cyber Agencies.
ITU: National CIRT Implementation Framework

NATIONAL CIRT IMPLEMENTATION, CAPACITY BUILDING AND OPERATIONS DEVELOPMENT PHASES
CIRT Benefits

National Awareness Strategy
Cyber Crime Legislation
National Identity and Access Management Framework
eGovernment Framework
Child Online Protection
Disaster Recovery Strategy

"Building Blocks" of the "National Cybersecurity Programme" within the Principles of "International Cooperation"

Enhanced Incident Response
Enhanced Incident Management
Culture of Cybersecurity
Prevention & Mitigation Strategy
Public-Private Sector Collaboration
National PKI

Human Capacity Building

Assist in Drafting the National Cybersecurity Strategy
The ITU Telecommunication Development Bureau (BDT) is facilitating the implementation process, managing communication and needs assessment with Member States and coordinating with IMPACT, to ensure effective delivery of the services provided.

**Global Response Centre**
- Global Early Warning System, detecting and monitoring cyber-threats

**National CIRT**
- Computer Incident Response Teams (CIRTs) and Incident Management capabilities at National level

**Capacity Building**
- *Capacity building and training*, on-site, on-line, and training on the job
- *Regional workshops and events*, to ensure sustainability and operations of the solutions
- *Direct assistance to countries*, to map the deployment with the needs of the Administration
How many children are using the Internet?

Proportion of Internet Users, by age and total (2008)

Source: ITU.
### Objectives

- Identify risks and vulnerabilities to children in cyberspace
- Create awareness
- Develop practical tools to help minimize risk
- Share knowledge and experience

### Child Online Protection (COP)

COP is a global initiative created by ITU, aims to tackle cybersecurity holistically, addressing legal, technical, organizational and procedural issues as well as capacity building and international cooperation

[www.itu.int/cop](http://www.itu.int/cop)
Guidelines on COP

ITU has been working with some COP members to develop initial sets of guidelines for the different stakeholders.

Guidelines for policy-makers
- Children’s Charities’ Coalition on Internet Safety (CHIS)
- United Nations Interregional Crime and Justice Research Institute (UNICRI)
- International Centre for Missing and Exploited Children (ICMEC)
- Child Helpline International (CHI)
- INTERPOL

Guidelines for industry
- Children’s Charities’ Coalition on Internet Safety (CHIS)
- GSM Association
- European Broadcasting Union (EBU)
- INTERPOL
- AfrISP
- Telecom Italia
- Vodafone

Guidelines for parents, guardians and educators
- Children’s Charities’ Coalition on Internet Safety (CHIS)
- University of Edinburgh, United Kingdom
- Insafe Network
- European Network and Information Security Agency (ENISA)
- European Commission’s Safer Internet programme
- Cyber Peace Initiative

Guidelines for children
- Telefónica
- Children’s Charities’ Coalition on Internet Safety (CHIS)
- Save the Children
- INTERPOL

http://www.itu.int/cop
COP National Strategy Guide

- Elaborated in cooperation with COP partners.
- The “Child Online Protection National Strategy Guide” assess the local status on the ground and presents a Country Action Plan for developing a national strategy based on the five pillars of the GCA.
COP Survey

- Carried out by the ITU, it aims to determine the scope of COP policy and legal frameworks across the world, establishing a database with issues faced at the national level.
- More than 90 countries have participated in the Survey. (Results available at ITU COP website)
• The Child Online Protection Statistical Framework and Indicators 2010 is the world’s first attempt on measuring child online protection in a country.

• It has particular emphasis on measures that allow international comparison.
COP Special Envoy & COP Patron

- 2010: Ms. Deborah Tate, US Former Federal Communications Commissioner, COP Special Envoy
- 2010: H.E. Laura Chinchilla (President of Costa Rica), the New COP Patron
International Initiatives

With the number of school girls opting to study technology-related disciplines on the decline in most countries worldwide, ITU is committed to championing the catalytic role a tech career can play in creating exciting, far-reaching opportunities for women and girls.

To help inspire girls to consider a future in technology, ITU established ‘Girls in ICT Day’ back in 2010 and supports the global organization of activities every year on the fourth Thursday in April. In only its third year, global momentum around Girls in ICT Day continues to grow with over 100 countries expected to hold events hosted by governments, private sector and NGOs in 2013.
Thank You!

For more information on ITU’s Cybersecurity Activities visit the website at: www.itu.int/cybersecurity/

or contact cybmail@itu.int