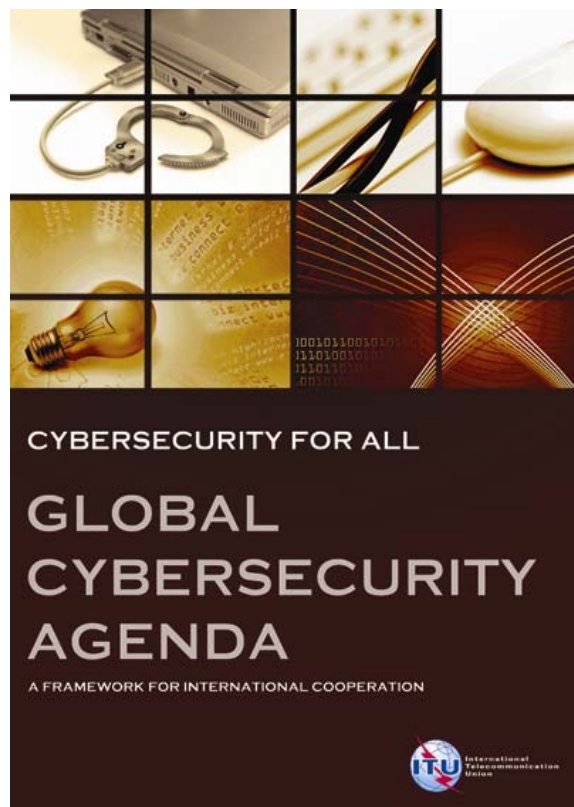

Cybersecurity for ALL



An Overview of ITU's Cybersecurity Activities

ITU Regional Cybersecurity Forum for Asia-Pacific

23 September 2009 in Hyderabad, India

Souheil Marine
Head, ICT Applications and Cybersecurity Division
ITU Telecommunication Development Bureau
souheil.marine@itu.int



Committed to connecting the world

Introduction to ITU

- Leading UN agency for information and communication technologies (ICT)
- Founded in 1865, ITU is the oldest specialized agency in the UN system
- Global focal point for governments and the private sector with 191 Member States, 900+ Sector Members and Associates
- ITU Headquarters in Geneva, 11 regional and area offices, 700 staff of 80 nationalities



Committed to connecting the world

ITU Activities

- ITU work is implemented through its three Sector's:

Standardization (ITU-T)

Radiocommunication (ITU-R)

Development (ITU-D)

- ITU also organizes TELECOM events:



ITU TELECOM WORLD 2009: an event for the global telecommunication and information communication technology (ICT) sector, and a platform for global telecommunications and ICTs

- ITU Website: www.itu.int/



Committed to connecting the world

Cybersecurity Issues and Challenges

- Constant evolution of the nature of cyber threats
- Vulnerabilities in software and hardware applications and services changing and increasing
- Countries are increasingly at risk and under attack
- Low entry barriers and increasing sophistication of the type of cybercrimes committed
- Loopholes in current legal frameworks
- Absence of appropriate national organizational structures to deal with the threats
- Inadequate cooperation amongst the various stakeholders and stakeholder groups



International
Telecommunication
Union

Committed to connecting the world

Global Cybersecurity Cooperation



The lack of cybersecurity is global problem that cannot be solved by any single entity alone!

The world is faced with the challenging task of developing harmonized and comprehensive strategies at the global and international level and implementing these with the various relevant national, regional, and international stakeholders in the countries



Committed to connecting the world

ITU and Cybersecurity

- ITU constitutes a unique global forum to discuss cybersecurity.
- The **ITU Secretary-General** has set **cybersecurity as a top priority**.
- **ITU Membership** has been calling for a **greater role to be played by ITU** in matters relating to cybersecurity through a number of Resolutions, Decisions, Programmes and Recommendations.
- ITU provides a global perspective and expertise and is promoting cybersecurity through a range of activities.





WSIS and Promoting a Global Culture of Cybersecurity

From WSIS Phase II: *Tunis Agenda*

39. We seek to build confidence and security in the use of ICTs by strengthening the trust framework. **We reaffirm the necessity to further promote, develop and implement in cooperation with all stakeholders a global culture of cybersecurity**, as outlined in UNGA Resolution 57/239 and other relevant regional frameworks.

This culture requires **national action** and **increased international cooperation** to strengthen security while enhancing the protection of personal information, privacy and data. Continued development of the culture of cybersecurity should enhance access and trade and must take into account the level of social and economic development of each country and respect the development-oriented aspects of the Information Society.



Committed to connecting the world



Global Framework for Cybersecurity: ITU's Global Cybersecurity Agenda

“Building confidence and security in the use of ICTs”

As a result, in 2007, ITU Secretary-General launched the **Global Cybersecurity Agenda**, an international framework for collaboration on cybersecurity matters that addresses **5 main areas**:

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



Committed to connecting the world

ITU-D's Work in Cybersecurity

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 ITU-D's 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 Conferences outcomes

Addressing the specific requirements of the countries,
to provide strategies at national level



Committed to connecting the world



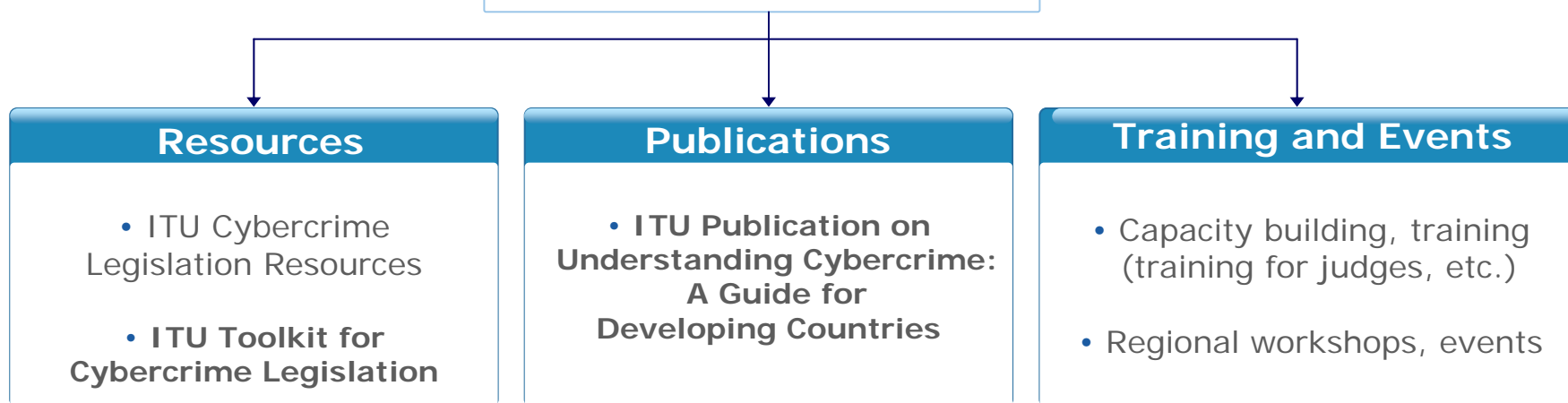
Legal Measures

■ 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



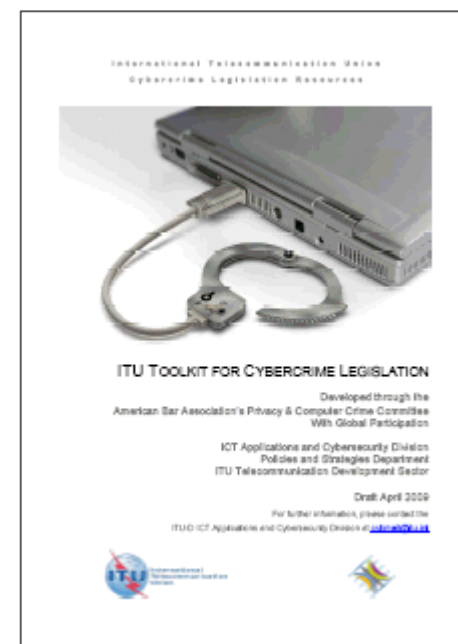
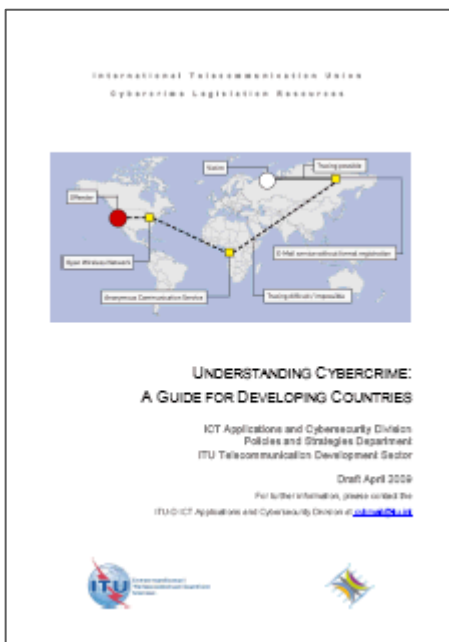
Committed to connecting the world



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



Committed to connecting the world



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



Committed to connecting the world



Cybersecurity Study Group Activities in ITU-T (Standardization)

- Focus on different topic areas
 - Security, access and transport networks, multimedia, signaling, numbering, naming and addressing, tariffs, IP and NGN
- Cooperation and collaborative activities with many organizations including regional telecom forums, IETF, ISO, IEC, ETSI, etc.
- Examples of specific ITU-T activities related to cybersecurity and Child Online Protection include:
 - **Study Group 17**
Primary focus on communication security
The Leading Study Group on security for ITU-T
 - **Study Group 2**
Operational aspects of service provision and telecommunication management works on harmonizing numbering resources for child helplines, etc.



Committed to connecting the world



Specific Cybersecurity Study Group Activities in ITU-T (Standardization)

- Study Group 17 has primary focus on communication security and is the Lead Study Group on security for ITU-T

Work under way under Study Group 17 Questions:

Working Party 1 Network and information security	Working Party 2 Application security	Working Party 3 Identity management/Languages
<p>Q 1 Telecommunications systems security project</p> <p>Q 2 Security architecture and framework</p> <p>Q 3 Telecommunications information security management</p> <p>Q 4 Cybersecurity</p> <p>Q 5 Countering spam by technical means</p>	<p>Q 6 Security aspects of ubiquitous telecommunication services</p> <p>Q 7 Secure application services</p> <p>Q 8 Telebiometrics</p> <p>Q 9 Service oriented architecture security</p>	<p>Q 10 Identity management architecture and mechanisms</p> <p>Q 11 Directory services, Directory systems, and public-key/attribute certificates</p> <p>Q 12 Abstract Syntax Notation One (ASN.1), Object Identifiers (OIDs) and associated registration</p> <p>Q 13 Formal languages and telecommunication software</p> <p>Q 14 Testing languages, methodologies and framework</p> <p>Q 15 Open Systems Interconnection (OSI)</p>





Other Cybersecurity Initiatives in ITU-T

- Correspondence group on exchange of network digital forensics
- Draft Recommendation on Traceback use cases and capabilities
- X.1240-series of Recommendations on technical means for countering spam
- Supplement 5 to ITU-T Recommendation E.164
- New Draft Recommendation on 'Specification of an Intl Numbering Resource for use in the provisioning of International Help lines'





Some Cybersecurity Initiatives in ITU-R (Radiocommunication)

- Radio spectrum global frequency management is increasingly important for building confidence and security and creating an enabling environment in the use of ICTs
- Some examples of ongoing activities include:
 - Recommendation ITU-R M.1457
"Security mechanism incorporated in IMT-2000"
 - Recommendation ITU-R M.1645
"Framework and overall objectives of the future development of IMT-2000 and systems beyond IMT-2000"
 - Recommendation ITU-R M.1223
"Evaluation of security mechanism for IMT-2000"
 - Recommendation ITU-R M.1078
"Security principles for IMT-2000"



Committed to connecting the world



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



ITU Secretary-General Dr Hamadoun Touré

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



International
Telecommunication
Union

Committed to connecting the world



ITU-IMPACT Alliance

Background Information

- ITU launched the Global Cybersecurity Agenda (GCA) as framework for international cooperation
- Within GCA, ITU and the International Multilateral Partnership Against Cyber-Threats (IMPACT) are pioneering the deployment of solutions and services to address cyber-threats on a global scale.
- In September 2008, ITU and IMPACT signed a Memorandum of Understanding (MoU)
- IMPACT's global headquarters in Cyberjaya, Malaysia becomes the physical home of the GCA.
- In March 2009 the global headquarters of IMPACT inaugurated by Malaysia's Prime Minister Dato' Seri Abdullah Haji Ahmad Badawi and ITU Secretary-General Dr Hamadoun Touré



Committed to connecting the world



ITU-IMPACT Alliance

Partners

Key intergovernmental organizations	Industry and academia	Leading cybersecurity training institutions
<ul style="list-style-type: none">▪ United Nations▪ International Police Organization INTERPOL▪ Etc.	<ul style="list-style-type: none">▪ Symantec Corporation▪ Kaspersky Lab▪ F-Secure Corporation▪ Trend Micro Inc.▪ Microsoft Corporation▪ Cisco Systems Inc.▪ Dell Inc.▪ Etc.	<ul style="list-style-type: none">▪ The SANS™ Institute▪ International Council of E-Commerce Consultants (EC-Council)▪ The Honeynet Project▪ (ISC)² Inc.



International
Telecommunication
Union



ITU-IMPACT Alliance

Goals

- Five pillars of the GCA mapped with the tracks identified by IMPACT:
 - **Legal Measures** - Elaborate strategies for the development of a model cybercrime legislation that is globally applicable and interoperable with existing national and regional legislative measures
 - **Technical and Procedural Measures** - Develop strategies for the creation of a global framework for watch, warning and incident response to ensure cross-border coordination between new and existing initiatives
 - **Organizational Structures** - Elaborate global strategies for the creation of appropriate national and regional organizational structures and policies on cybercrime
 - **Capacity Building** - Develop a global strategy to facilitate human and institutional capacity building to enhance knowledge and know-how across sectors and in all the above-mentioned areas
 - **International Cooperation** - Propose a framework for a global multi-stakeholder strategy for international cooperation, dialogue and coordination in all the above-mentioned areas



Committed to connecting the world



ITU-IMPACT Alliance

Status of Collaboration

- **Thirty countries joined the ITU-IMPACT collaboration:**

Afghanistan, Andorra, Brazil, Bulgaria, Burkina Faso, Costa Rica
Cote D'Ivoire, Democratic Republic of Congo, Egypt, Ghana, India
Indonesia, Iraq, Israel, Kenya, Lao, Malaysia, Mauritius, Montenegro
Morocco, Nepal, Nigeria, Philippines, Saudi Arabia, Serbia, Seychelles
Syrian Arab Republic, Tunisia, Uganda, United Arab Emirates and
Zambia



- By the end of September 2009, all Member States that have confirmed their participation will be able to access the Global Response Center (GRC).
- **The Africa Region has been identified this activity started together with the ITU-EC project**
 - Starting with ten countries in the region:
Burundi, Burkina Faso, Cote D'Ivoire, Ghana, Kenya, Nigeria, Rwanda, Tanzania, Uganda and Zambia





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

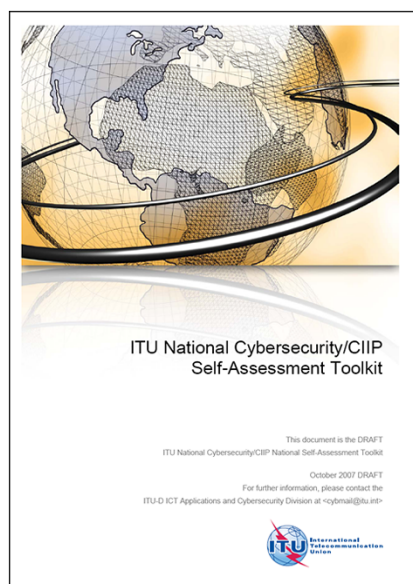
- Capacity building and training across all the pillars of the GCA
- Targeted workshops and events



Committed to connecting the world



Examples of Some Ongoing Initiatives



ITU National Cybersecurity/CIIP Self-Assessment Tool

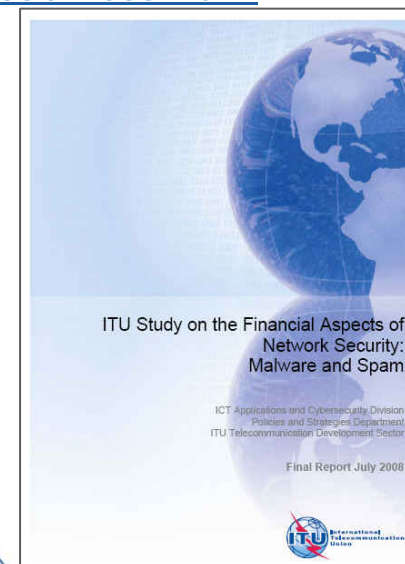
To assist governments in examining existing national policies, procedures, norms, institutions and other elements necessary for formulating cybersecurity strategies

- www.itu.int/ITU-D/cyb/cybersecurity/readiness.html

ITU Study on the Financial Aspects of Network Security: Malware and Spam, 2008

The study develops a framework within which the financial impacts and implications can be assessed and brings together the many disparate sources of financial data on malware and spam.

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



**International
Telecommunication
Union**

Committed to connecting the world

Examples of Some Ongoing Initiatives



ITU Regional Cybersecurity Forums

8 regional cybersecurity events held in 2007 and 2008 in all regions.
Several more planned for 2009.

- **ITU Regional Cybersecurity Forum for Europe and CIS** held in Bulgaria, 7-9 October 2008
- **2009 ITU Regional Cybersecurity Forum for Africa and Arab States** held in Tunisia, 4-5 June 2009
- **2009 ITU Regional Cybersecurity Forum for Asia Pacific** being held in India, 23-25 September 2009

- www.itu.int/ITU-D/cyb/events/



Committed to connecting the world



International Cooperation

■ 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



International
Telecommunication
Union

Committed to connecting the world

Child Online Protection



Child Online Protection (COP)

- COP is a global initiative created by ITU, as part of the Global Cybersecurity Agenda, aims to address cybersecurity holistically.

COP Objectives:

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

- www.itu.int/cop/



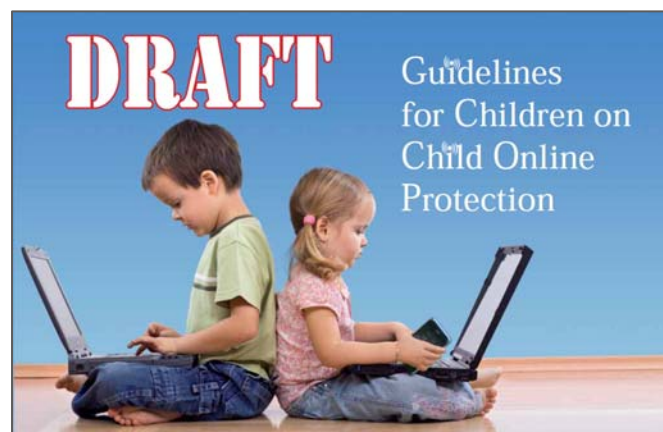
International
Telecommunication
Union

Committed to connecting the world



Child Online Protection (COP) Guidelines

- Guidelines for Children
- Guidelines for Parents, Guardians and Educators
- Guidelines for Industry
- Guidelines for Policy Makers



The Draft Guidelines can be found online at:
www.itu.int/COP

- The revised Guidelines will be presented in October 2009
at **ITU TELECOM WORLD 2009**

Links to 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 National Cybersecurity/CIIP Self-Assessment Toolkit
 - www.itu.int/ITU-D/cyb/projects/readiness.html
- ITU Cybercrime Legislation Resources
 - www.itu.int/ITU-D/cyb/cybersecurity/legislation.html
- ITU Botnet Project Website
 - www.itu.int/ITU-D/cyb/cybersecurity/projects/botnet.html
- Regional Cybersecurity Forums and Conferences
 - www.itu.int/ITU-D/cyb/events/
- ITU Child Online Protection (COP)
 - www.itu.int/cop/



Committed to connecting the world

Thank You!

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

or contact cybmail@itu.int



Committed to connecting the world