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

Acknowledgements and Contact Information

The *ITU Cybersecurity Work Programme to Assist Developing Countries* was elaborated by the ICT Applications and Cybersecurity Division, Policies and Strategies Department, ITU Telecommunication Development Sector. A number of internal and external contributors and reviewers have assisted in refining this document and appreciation is extended to them.

The *ITU Cybersecurity Work Programme to Assist Developing Countries* is regularly updated to reflect the changing needs of the ITU membership and experience gained.

The latest version of this document is available at:

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

For further information on this document, please contact:

ICT Applications and Cybersecurity Division
Policies and Strategies Department
Telecommunication Development Sector
International Telecommunication Union
Place des Nations
1211 Geneva 20
Switzerland

Telephone: +41 22 730 5825/6052
Fax: +41 22 730 5484
E-mail: cybmail@itu.int
Website: www.itu.int/ITU-D/cyb/

1. Table of Contents

2. Executive Summary

This document, the *ITU Cybersecurity Work Programme to Assist Developing Countries*[1] (hereafter "*Cybersecurity Work Programme*"), was elaborated by the ICT Applications and Cybersecurity Division, Policies and Strategies Department, ITU Telecommunication Development Bureau (BDT). The document begins with background on the topic of cybersecurity and refers to related ITU mandates and resolutions from the ITU Plenipotentiary Conference (Antalya, 2006) and World Telecommunications Development Conference (Doha, 2006). This document then scopes out a set of high level assistance activities for developing countries, with each activity containing a set of more detailed initiatives to be undertaken in the 2007-2009 work period. Following an internal review process, the *Cybersecurity Work Programme* has been reflected in the BDT Operational Plan for Programme 3[2] of the 2006 World Telecommunication Development Conference's Doha Action Plan[3].

An executive summary of the high level assistance activities planned for 2007-2009 includes:

- General Management and Coordination
- ITU Member States' Cybersecurity Requirements and Mutual Assistance Capabilities
- National Strategies and Capabilities
- Legislation and Enforcement Mechanisms
- Watch, Warning and Incident Response (WWIR) Capabilities
- Countering Spam and Related Threats
- Bridging the Security-Related Standardization Gap
- Project on Enhancing Cybersecurity and Combating Spam
- Cybersecurity Indicators

[1] http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-cybersecurity-work-programme-developing-countries.pdf

[2] http://www.itu.int/ITU-D/cyb/publications/2006/dohaactionplanprogramme3.pdf

[3] http://www.itu.int/ITU-D/wtdc06/pdf/dohaactionplan.pdf

- Fostering Regional Cooperation Activities
- Information Sharing and Supporting the ITU Cybersecurity Gateway
- Outreach and Promotion

A consolidated list of all detailed initiatives under these high level assistance activities can be found in *Annex A: Overview of Detailed Initiatives* on page 59.

3. Introduction and Overview

3.1. Our Growing Dependencies on Networked Information and Communication Technologies

With the start of the 21st century, modern societies have a growing dependency on information and communication technologies (ICTs) that are globally networked. However, with this growing dependency, new threats to network and information security have emerged. There is a growing misuse of electronic networks for criminal purposes or for objectives that can adversely affect the integrity of national critical information infrastructures. To address these threats and to protect these infrastructures, a coordinated National Cybersecurity Strategy and Critical Information Infrastructure Protection (CIIP) programme is necessary.

3.2. The Issues Become Global

As threats can originate anywhere around the globe, the scope of the problem is inherently international and the topic has entered the global political agenda. Examples include:

- In 2002 and 2004, UN Resolutions 57/239 and 58/199 on the *Creation of a global culture of cybersecurity* and *Creation of a global culture of cybersecurity and the protection of critical information infrastructures* were adopted.
- Between 1997-2001, the Council of Europe's *Convention on Cybercrime* was negotiated and opened for signature and ratification by States.
- Following the World Summit on the Information Society (WSIS), ITU was requested to play the facilitator/moderator role for WSIS Action Line C5: Building Confidence and Security in the Use of ICTs.
- ITU's World Telecommunication Development Conference (WTDC-06) initiated the four year *Study Group Question 22/1: Securing information and communication networks: Best practices for developing a culture of cybersecurity*, adopted Resolution 45 (Doha 2006) on *Mechanisms for enhancing cooperation on cybersecurity, including combating spam*, and defined the scope of Programme 3's cybersecurity-related priorities, tasks and assistance to members.
- ITU's Plenipotentiary *Resolution 130: Strengthening the role of ITU in building confidence and security in the use of information and communication technologies*, adopted in 2002 and updated at the 2006 Plenipotentiary Conference, instructs the Secretary-General and Directors of the Bureaux to give this work a high priority within ITU.
- The ITU Secretary-General's *Global*

Cybersecurity Agenda launched in 2007.

3.3. What is in this Document?

This document is the *ITU Cybersecurity Work Programme to Assist Developing Countries* (hereafter "*Cybersecurity Work Programme*") prepared by the ICT Applications and Cybersecurity Division, Policies and Strategies Department, ITU Telecommunication Development Bureau (BDT).

This document scopes out a set of proposed high level cybersecurity assistance activities to assist developing countries with each activity containing a set of more detailed initiatives planned to be undertaken in the 2007-2009 work period by the ICT Applications and Cybersecurity Division (CYB).

Following an internal review process, the *Cybersecurity Work Programme* has been reflected in the BDT Operational Plan for Programme 3[4] of the 2006 World Telecommunication Development Conference's Doha Action Plan[5].

Key related ITU Resolutions on Cybersecurity are listed in *Annex B: ITU Resolutions Relating to Cybersecurity* on page 71.

3.4. How to Use this Document

Each section of this document begins with a high level assistance activity followed by subsections describing detailed initiatives. Each initiative includes the following elements:

- Title of the Initiative
- Objective
- Activity Description
- Deliverables
- Partners
- Priority (high/medium/low)
- Deadlines
- Promotion and Events
- Resources (staff and budget)
- Reference Material
- Related ITU Plenipotentiary Conference and/or WTDC-06 Mandate
- Related BDT Operational Plan Action Line(s)

A consolidated list of detailed initiatives can be found in *Annex A: Overview of Detailed Initiatives* on page 59.

[4] http://www.itu.int/ITU-D/cyb/publications/2006/dohaactionplanprogramme3.pdf

[5] http://www.itu.int/ITU-D/wtdc06/pdf/dohaactionplan.pdf

4. General Management and Coordination

Background Information: This section discusses the *Cybersecurity Work Programme* general management and coordination tasks.

4.1. General Management and Coordination Activities

Objective: To assist developing countries in cybersecurity, the activities to be undertaken involve a number of Programme 3 administrative activities to support both the detailed initiatives described in this document as well as the related ITU-D Study Group 1 Question 22 activities. The *ICT Applications and Cybersecurity Division (CYB)* has the primary responsibility in BDT for supporting ongoing cybersecurity and countering spam activities. In particular, these activities include the preparation and maintenance of the *Cybersecurity Work Programme*, facilitating cooperation of ITU with organizations involved in promoting global cybersecurity (see *Annex C: Organisations Involved in Cybersecurity Initiatives* on page 89), responding to requests for assistance from ITU Member States, maintaining and enhancing the Division's website for information sharing on related Programme 3 initiatives, making maximum use of online tools for supporting relationship with partners and ITU Member States, managing related mailing lists/forums for information sharing and planning, managing contact and directory information, coordinating publications, conducting surveys, responding to correspondence, planning and organizing events at ITU Headquarters and in the regions (in cooperation with ITU regional offices), and conducting reviews of key deliverables and reporting functions.

A key role of CYB involves developing and maintaining relationships with relevant actors (see *Annex C: Organisations Involved in Cybersecurity Initiatives* on page 89), identifying common areas of interest, and assessing to which extent collaboration with such actors in specific activities of the BDT are desirable and possible. In addition, there are close synergies that have been developed with work underway in ITU-D Study Group Question 22/1: *Securing information and communication networks: Best practices for developing a culture of cybersecurity* and the *Cybersecurity Work Programme.* In particular, a number of activities in this Document are intended to support Question 22/1 related activities (e.g., the ITU National Cybersecurity/CIIP Self Assessment Toolkit described in Section 6.4). The

Cybersecurity Work Programme also supports activities undertaken in ITU-T Study Group 17, the ITU-T Lead Study Group on Telecommunication Security as well as supporting ITU's WSIS Action Line C5 facilitation role for implementation activities under this Action Line.

5. ITU Member States’ Cybersecurity Requirements and Mutual Assistance Capabilities

Background Information: ITU’s commitment to assist developing countries is being implemented through two key and interrelated pillars. The first pillar is a new ITU Telecommunication Development Sector Study Group 1 Question 22 entitled “*Securing information and communication networks: Best practices for developing a culture of cybersecurity*”. In this activity, ITU is developing a *Report on Best Practices for a National Approach to Cybersecurity*. This *Report* outlines a *Framework for Organizing a National Approach to Cybersecurity* that identifies five key elements of a national effort, including: 1) Developing a national cybersecurity strategy; 2) Establishing national government-industry collaboration; 3) Creating a national incident management capability; 4) Deterring cybercrime; and 5) Promoting a national culture of cybersecurity. The second interrelated pillar is the *ITU Cybersecurity Work Programme for Developing Countries* which sets out a detailed agenda how the Development Sector plans to assist Member States in developing cybersecurity capacities during the 2007-2009 timeframe.

5.1. Review of ITU Member States’ Requirements and Mutual Assistance Capabilities

Objective: Understand and document Member States’ needs in the area of cybersecurity, develop framework model, provide tools/toolkits to assist in the elaboration of national strategies and other key topics, establish key contacts.

Activity Description: This activity involves gaining an appreciation of Member State needs assessment in a number of high-level areas, while gathering information on Member States who may be able to offer assistance through peer capabilities. This activity includes: summarizing these high level framework needs (e.g., confirming the high level activities in this document); collecting and analyzing the data gathered; making specific proposals for detailed and practical initiatives; and making contacts and/or arrangements for hosting of related activities and/or peer assistance. An important goal of this work is to establish key regional contacts to provide catalyst/ leadership roles in regions, including possible hosts for regional events or as catalysts for eventual regional cooperation frameworks.

Deliverables:

1) Map ITU-D Study Group 22/1 framework activities against framework model activities in this document. Development of strategy to reach maximum number of Member States for both awareness raising and targeted capacity building;

2) ITU National Cybersecurity/CIIP Self Assessment Toolkit;

3) Establishment of a list of key national and regional cybersecurity contact points based on information provided by Member States .

Partners: ITU Member States, ITU Regional Offices

Priority: High

Deadlines: Ongoing assessment of Member States' needs in cybersecurity and countering spam 2007, 2008, 2009

Promotion and Events: Deliverables related to this activity to be presented at most ITU events

Resources (staff and budget): ITU/BDT/POL/CYB internal resources

Reference Material: Information in the ITU Cybersecurity Gateway on services currently available in Member States (also included contributions submitted by Member States in 2006).

Related ITU Plenipotentiary Conference and/or WTDC-06 Mandate : Res. 130 (Rev. Antalya, 2006)

Related BDT Operational Plan Action Line(s): 9167 (2007), 9819, 10038 (2008), 9844 (2009)

6. National Strategies and Capabilities

Background Information: 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. Developing countries, with limited human, institutional and financial resources, face particular challenges in elaborating and implementing national policies and frameworks for cybersecurity and CIIP. For this reason, at the World Telecommunication Development Conference 2006 held in Doha, Qatar, cybersecurity was designated as a top priority for the ITU Telecommunication Development Sector (ITU-D). 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 between the government authorities, the private sector and citizens, requiring coordinated action related to the prevention, preparation, response, and recovery from incidents. At the regional and international level, this entails cooperation and coordination with relevant partners. The formulation and implementation of a framework for cybersecurity and critical information infrastructure protection requires a comprehensive approach involving all parties.

6.1. Identification of Best Practices in the Establishment of National Frameworks for Cybersecurity and CIIP

Objective: Provide Member States with a concrete framework to consider when elaborating a national strategy for cybersecurity and CIIP.

Activity Description: To support ITU's activities in the domain of cybersecurity and CIIP, there needs to be research and development of a best practices framework for cybersecurity and CIIP which can be adopted and adapted to national needs. The ITU Telecommunication Development Sector's Study Group 1 Question 22 entitled "*Securing information and communication networks: Best practices for developing a culture of cybersecurity*" is working to develop a *Report on Best Practices for a National Approach to Cybersecurity*. The draft *Report* (September 2007 version) outlines a *Framework for Organizing a National Approach to Cybersecurity* that identifies five key elements of a national effort, including: 1) Developing a national cybersecurity strategy; 2) Establishing national government-industry collaboration; 3) Creating a national incident management capability; 4) Deterring cybercrime; and 5) Promoting a national culture of cybersecurity.

Deliverables: Contributions towards successful delivery of the ITU-D Study Group 1 Question 22 *Report on National Best Practices Framework for Cybersecurity and CIIP*.

Partners: ITU-D Study Group 1 Question 22, other relevant ITU parties

Priority: High

Deadlines: Study Group 1 Question 22 has a four year study cycle (2006-2010)

Promotion and Events: Deliverables related to this activity to be presented at most ITU events

Resources (staff and budget): ITU/BDT/POL/CYB internal resources

Reference Material: ITU-D Question 22/1: Securing information and communication networks: Best practices for developing a culture of cybersecurity resources, CRN International CIIP Handbook: An Inventory and Analysis of National Protection Policies.

Related ITU Plenipotentiary Conference and/or WTDC-06 Mandate: Res. 130 (Rev. Antalya, 2006)

Related BDT Operational Plan Action Line(s): 9757(2007), 9819 (2008), 9844 (2009) and 10038 (2008) and indirectly related to 2007 workshop related actions: 9031, 9718, 9757, 10096; 2008 workshop related actions: 9815, 9904, 9939, 10039, 10179; and 2009 actions 9941, 10041 (Unfunded), 10170

6.2. Country Case Studies for Best Practices in the Establishment of National Frameworks for Cybersecurity and Critical Information Infrastructure Protection

Objective: Showcase different national experiences in developing national frameworks for cybersecurity and critical information infrastructure protection.

Activity Description: To develop and present case studies of national experiences in creating frameworks for cybersecurity and critical information infrastructure protection.

Deliverables: Case studies showing experiences in developing and implementing national frameworks for cybersecurity and critical information infrastructure protection.

Partners: TBD

Priority: Low

Deadlines: December 2008

Promotion and Events: TBD

Resources (staff and budget): ITU/BDT/POL/CYB internal resources

Reference Material: ITU-D Question 22/1: *Securing information and communication networks: Best practices for developing a culture of cybersecurity* resources, CRN International CIIP Handbook: An Inventory and Analysis of National Protection Policies.

Related ITU Plenipotentiary Conference and/or WTDC-06 Mandate: Res. 130 (Rev. Antalya, 2006)

Related BDT Operational Plan Action Line(s): TBD

6.3. Regional Workshops/Forums on Frameworks for Cybersecurity and CIIP

Objective: Ensure that developing countries develop a good understanding of the components that are needed to formulate and implement a comprehensive framework for cybersecurity and critical information infrastructure protection.

Activity Description: Organization of regional capacity building workshops/forums on frameworks for cybersecurity and critical information infrastructure protection.

Deliverables: Delivery of regional workshops/forums on frameworks for cybersecurity and critical information infrastructure protection.

Partners: Regional offices, relevant TSB parties, and organizations with specific mandate and expertise as well as subject matter experts.

Priority: High

Deadlines: 2007 workshops/forums on frameworks for cybersecurity and CIIP in Asia-Pacific (August 2007), the Americas (October 2007), and West Africa (November 2007). 2008 and 2009 workshops/forums organized across the ITU regions.

Promotion and Events: In 2007 workshops/forums were held in Asia-Pacific (Hanoi, Vietnam), the Americas (Buenos Aires, Argentina) and West Africa (Praia, Cape Verde). Additional regional workshops/forums are planned for 2008 and 2009 (Doha, Qatar; Sofia, Bulgaria), etc.

Resources (staff and budget): ITU/BDT/POL/CYB internal resources

Reference Material: Information on planned and implemented workshops/forums can be found at http://www.itu.int/ITU-D/cyb/events/.

Related ITU Plenipotentiary Conference and/or WTDC-06 Mandate: Res. 130 (Rev. Antalya, 2006) TBD

Related BDT Operational Plan Action Line(s): 2007 workshop related actions: 9031, 9718, 9757, 10096; 2008 workshop related actions: 9815, 9904, 9939, 10039, 10179; 2009 workshop related actions 9941, 10041 (Unfunded), 10170

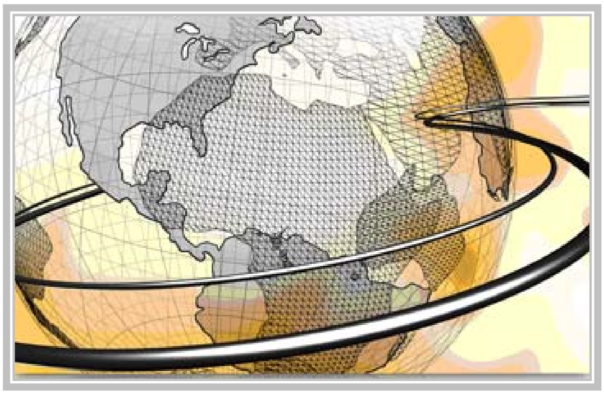
6.4. National Cybersecurity/CIIP Readiness Self-Assessment Toolkit

Objective: Increase Member States' cybersecurity awareness and allow countries to self-assess national cybersecurity/CIIP readiness with the help of a dedicated and easy to use toolkit.

Activity Description: Develop a national cybersecurity/CIIP readiness self-assessment toolkit for use by developing countries to assist them in the elaboration of national cybersecurity policies. More specifically, the toolkit is intended to assist national governments to examine their existing national policies, procedures, norms, institutions, and relationships in light of the evolving changes in information and communication technologies, the requirements of critical information infrastructure and the need to enhance cybersecurity. The toolkit examines these issues at the policy and management levels and should be considered in the context of the report on *Best Practices for a National Approach to Cybersecurity* and the *Framework for Organizing a National Approach to Cybersecurity* therein being developed through the work of ITU-D Study Group 1 Question 22. The methodology used is to enable users to be independently guided toward consistent approaches, responses, and outputs. The toolkit can function as a checklist to guide national activities and the development of national strategies. It can also be used as a survey tool to assess cybersecurity approaches, identify regional or country deficiencies and furthermore to guide educational programs and security curriculum development.

The methodology includes a standard template containing assessment components and factors in the following areas, (including international coordination and cooperation in these areas):

- *National Strategy for Cybersecurity* (i.e. government organization for cybersecurity and critical information infrastructure protection, including government policies, etc.);
- *Government-Industry Collaboration* (including public-private sector interaction and coordination for cybersecurity);
- *Deterring Cybercrime* (including the establishment of a legal framework to deal with criminalizing the misuse of ICTs, cybercrime, privacy and cybersecurity issues, as well as international cooperation in this domain);
- *Incident Management Capabilities* (including organizational structures and incident response capabilities, the establishment of Computer Emergency Response Teams (CERTs), Computer Security Incident Response Team (CSIRTs), Information Sharing And Analysis Centers (ISACs), and enhancement of law enforcement capabilities); and



- *Culture of Cybersecurity* (including education, awareness raising and specific training);

Deliverables: Toolkit and related training material for Member States.

Partners: ITU-D Study Group 22/1, and other relevant entities, organizations, etc.

Priority: High

Deadlines: Draft toolkit available on August 2007, revised version on October 2007, and further revised version on early 2008. First pilot project in Vietnam, August 2007, second pilot project in Argentina, October 2007, third pilot project in Qatar, February 2008.

Promotion and Events: TBD

Resources (staff and budget): ITU/BDT/POL/CYB internal resources, external experts, ITU Area and Regional Offices

Reference Material: Information on elements of the toolkit can be found at http://www.itu.int/ITU-D/cyb/cybersecurity/projects/readiness.html.

Related ITU Plenipotentiary Conference and/or WTDC-06 Mandate: Res. 130 (Rev. Antalya, 2006)

Related BDT Operational Plan Action Line(s): 9167 (2007), 9819 (2008), 10038 (2008), 9844 (2009)

6.5. Pilot Projects in ITU Member States for Implementation of the National Cybersecurity/CIIP Readiness Self-Assessment Toolkit

Objective: Allow and enable Member States to self-assess national cybersecurity/CIIP readiness with the help of a dedicated toolkit.

Activity Description: The purpose of the national cybersecurity/CIIP readiness self-assessment toolkit is to help national governments to examine their existing national policies, procedures, norms, institutions, and relationships in light of the evolving changes in information and communication technologies, the requirements of critical information infrastructure and the need to enhance cybersecurity. To ensure that the toolkit meets the needs of the Member States, a number of pilot projects are conducted. The pilot projects provide training and expert assistance to selected Member States and simultaneously provide a means to assess the usefulness of the tool, and make necessary changes to the toolkit to reflect the specific needs of developing countries when establishing a comprehensive national cybersecurity/CIIP strategy.

Deliverables: Implementation of pilot projects in the Member States.

Partners: ITU-D Study Group 22/1, and other relevant entities, organizations, etc.

Priority: High

Deadlines: First pilot project in Vietnam, August 2007, second pilot project in Argentina, October 2007, third pilot project in Qatar, February 2008. For 2008 and 2009, pilot self-assessments are planned for countries in Africa, Arab States, Asia Pacific, Americas, and Europe/CIS.

Promotion and Events: TBD

Resources (staff and budget): ITU/BDT/POL/CYB internal resources, ITU Area and Regional Offices

Reference Material: Information on elements of the toolkit can be found at http://www.itu.int/ITU-D/cyb/cybersecurity/projects/readiness.html.

Related ITU Plenipotentiary Conference and/or WTDC-06 Mandate: Res. 130 (Rev. Antalya, 2006)

Related BDT Operational Plan Action Line(s): 6167 (2007), 10038 (2008), 9844 (2009)

6.6. Online Cybersecurity Forum to Help Developing Countries Build Capacity

Objective: Increase the level of communication and expertise amongst cybersecurity professionals and other interested stakeholders.

Activity Description: The purpose of the online cybersecurity forum is to help developing countries develop capacity in the different areas related to cybersecurity and countering spam. The forum gathers experts from both developed and developing countries to exchange ideas on specific cybersecurity and CIIP related topics.

Deliverables: Implementation of an online cybersecurity forum

Partners: ITU-D Study Group 22/1, other relevant entities within ITU, external experts to help moderate the online forum.

Priority: Medium

Deadlines: Launch of forum in 2008, forum to be further enhanced in 2009

Promotion and Events: TBD

Resources (staff and budget): ITU/BDT/POL/CYB internal resources

Reference Material: To be added

Related ITU Plenipotentiary Conference and/or WTDC-06 Mandate: Res. 130 (Rev. Antalya, 2006)

Related BDT Operational Plan Action Line(s): 9764 (2008), 9843 (2009)

6.7. Toolkit for Promoting a Culture of Cybersecurity

Objective: Capacity building to raise awareness of the value of promoting a culture of cybersecurity in all ITU Member States.

Activity Description: The toolkit aims to raise awareness on numerous cybersecurity issues for small and medium sized enterprises (SMEs), consumers and end-users in developing countries.

Deliverables: Toolkit for promoting a culture of cybersecurity and delivery of related awareness raising activities/materials

Partners: ITU-D Study Group Q22/1, other entities within ITU, external experts.

Priority: Medium

Deadlines: December 2009

Promotion and Events: TBD

Resources (staff and budget): ITU/BDT/POL/CYB internal resources

Reference Material: To be added

Related ITU Plenipotentiary Conference and/or WTDC-06 Mandate: Res. 130 (Rev. Antalya, 2006)

Related BDT Operational Plan Action Line(s): 9821, 9836 (2009)

6.8. Online Training Modules for Cybersecurity Awareness and Solutions

Objective: Increase the level of awareness of cybersecurity issues and propose best practice approaches for ITU Member States.

Activity Description: Develop online training modules for cybersecurity awareness, challenges and solutions in collaboration with external partners and ITU Centres of Excellence.

Deliverables: Delivery of online training modules for raising awareness on cybersecurity and CIIP

Partners: ITU Centers of Excellence, ITU-D Study Group 22/1, other relevant entities within ITU, and external experts and entities.

Priority: Medium

Deadlines: Ongoing 2008, 2009

Promotion and Events: TBD

Resources (staff and budget): ITU/BDT/POL/CYB internal resources

Reference Material: To be added

Related ITU Plenipotentiary Conference and/or WTDC-06 Mandate: Res. 130 (Rev. Antalya, 2006)

Related BDT Operational Plan Action Line(s): 9818 (2009)

7. Legislation and Enforcement Mechanisms

Background Information: 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 infrastructures. As threats can originate anywhere around the globe, the challenges are inherently international in scope, and it is desirable to raise awareness of international best practices and facilitate regional and international cooperation.

7.1. Regional Capacity Building Activities on Cybercrime Legislation and Enforcement

Objective: Increase awareness in ITU Member States on the importance of cybercrime legislation and related enforcement.

Activity Description: Organization of regional capacity building activities on cybercrime legislation and related enforcement.

Deliverables: Regional and global workshops/forums on frameworks for cybersecurity and CIIP with focus on capacity building on cybercrime legislation and enforcement, related training material (CD-ROMs, websites, publications, etc.).

Partners: Council of Europe, UNODC, other relevant regional and international organizations, national justice ministries

Priority: High

Deadlines: Ongoing 2007 and 2008

Promotion and Events: In 2007: one event in the Asia-Pacific (Vietnam), one in the Americas (Argentina), and one in West Africa (Cape Verde). For 2008 and 2009 regional workshops/forums are planned for countries in Africa, Arab States, Asia Pacific, Americas, and Europe/CIS.

Resources (staff and budget): ITU/BDT/POL/CYB internal resources

Reference Material: To be added

Related ITU Plenipotentiary Conference and/or WTDC-06 Mandate: Res. 130 (Rev. Antalya, 2006)

Related BDT Operational Plan Action Line(s): 2007 workshop related actions: 9031, 9718, 9757, 10096;
2008 workshop related actions: 9815, 9824 (Unfunded), 9904, 9939, 10039, 10179;
and 2009 actions 9846 (Unfunded), 9941, 10041 (Unfunded), 10170

7.2. Revision of Existing Cybersecurity Publication and Launch of Publication on Understanding Cybercrime

Objective: Deliver an up-to-date revision of the ITU publication “Cybersecurity Guide for Developing Countries” and share information on threats to cybersecurity through a new publication on cybercrime.

Activity Description: Deliver an up-to-date revision of the existing ITU publication “Cybersecurity Guide for Developing Countries”. This activity also includes the delivery of a new publication dedicated to helping countries better understand cybercrime (title to be defined).

Deliverables: Revised Cybersecurity Guide for Developing Countries publication and launch of new publication to help countries better understand cybercrime

Partners: External expert with peer review by representatives from relevant international, regional, and national entities, including interested representatives of national justice ministries.

Priority: High

Deadlines: Q1 2008

Promotion and Events: Regional workshops/forums on frameworks for cybersecurity and CIIP

Resources (staff and budget): ITU/BDT/POL/CYB internal resources

Reference Material: The current version of the 2007 Cybersecurity Guide for Developing Countries publication is available online on CYB website in all six official U.N. languages.

Related ITU Plenipotentiary Conference and/or WTDC-06 Mandate: Res. 130 (Rev. Antalya, 2006)

Related BDT Operational Plan Action Line(s): 9167 (2007)

7.3. Toolkit for Cybercrime Legislation for Developing Countries

Objective: Provide countries with reference material that can assist in the establishment of a legislative framework to deter cybercrime.

Activity Description: Additional reference material for cybercrime legislation is needed to assist developing countries in the development of their legal frameworks for cybersecurity and to promote harmonization towards international best practices in combating cybercrime. Representing one of the five elements identified in the ITU-D Study Group Q22/1 developed Framework for Organizing a National Approach to Cybersecurity, deterring cybercrime is an integral component of a national cybersecurity/CIIP strategy. In particular, this includes the adoption of appropriate legislation against the misuse of ICTs for criminal or other purposes and activities intended to affect the integrity of national critical infrastructures. As threats can originate anywhere around the globe, the challenges are inherently international in scope and it is desirable to promote harmonization towards international best practices in combating cybercrime. The *ITU Toolkit for Cybercrime Legislation* aims to provide countries with reference material that can assist in the establishment of a legislative framework to deter cybercrime. Development of the toolkit is being undertaken by a multidisciplinary international group of experts and a first draft will be made available in the first quarter of 2008.

Deliverables: Toolkit to assist countries in the establishment of a legislative framework to deter cybercrime and aid countries when drafting cybercrime related legislation.

Partners: Multidisciplinary and international group of experts, with peer review by international experts.

Priority: High

Deadlines: March 2008

Promotion and Events: Toolkit will be promoted at all ITU events that deal with the issue of cybersecurity and deterring cybercrime.

Resources (staff and budget): ITU/BDT/POL/CYB internal resources

Reference Material: N/A

Related ITU Plenipotentiary Conference and/or WTDC-06 Mandate: Res. 130 (Rev. Antalya, 2006), WTDC Programme 3

Related BDT Operational Plan Action Line(s): 9172 (2007), 9824 (Unfunded), 9826 (Unfunded) (2008), 9846 (Unfunded) (2009)

7.4. Cybersecurity Module in the ITU/InfoDev ICT Regulation Toolkit

Objective: Provide developing countries with high quality information assistance on cybersecurity threats and issues through a specific cybersecurity module in the ITU/InfoDev ICT Regulation Toolkit.

Activity Description: Develop a complementary module on cybersecurity and countering spam, within the ITU/InfoDev ICT Regulation Toolkit (available at http://www.ictregulationtoolkit.org)

Deliverables: Online toolkit/module aligned with the regulation toolkit.

Partners: BDT Programme 1, external experts, etc.

Priority: Medium

Deadlines: December 2009

Promotion and Events: Toolkit will be promoted at all ITU events that deal with the issue of cybersecurity.

Resources (staff and budget): ITU/BDT/POL/CYB internal resources

Reference Material: ITU/InfoDev ICT Regulation Toolkit available at http://www.ictregulationtoolkit.org

Related ITU Plenipotentiary Conference and/or WTDC-06 Mandate: Res. 130 (Rev. Antalya, 2006)

Related BDT Operational Plan Action Line(s): 9766 (Unfunded)(2008)

8. Watch, Warning and Incident Response (WWIR) Capabilities

Background Information: 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.

8.1. Assistance to Developing Countries Related to Establishment of Watch, Warning and Incident Response (WWIR) Capabilities

Objective: Provide assistance to developing countries in establishing Computer Security Incident Response Teams (CSIRTs)/Computer Emergency Response Teams (CERTs)/ Warning, Advice and Reporting Points (WARPs) with the overall objective of assisting nations organize and manage national efforts to prevent, prepare for, protect against, respond to, and recover from cybersecurity incidents.

Activity Description: Creation of a CSIRT toolkit and dedicated websites to provide assistance to developing countries in establishing Watch, Warning and Incident Response (WWIR) capabilities which can include targeted assistance to set up national/regional CSIRT/CERTS/WARPs/etc. The activity includes dedicated regional workshops/forums for enhancing national capacity related to watch, warning, and incident response.

Deliverables: Toolkit for establishing CSIRT/CERTS/WARPs/etc., delivery of workshops/forums.

Partners: FIRST, ENISA, CERT/CC, Carnegie Mellon University Software Engineering Institute (SEI), National and Regional CSIRTs

Priority: Medium

Deadlines: Ongoing 2008 and 2009

Promotion and Events: Regional workshops/forums on frameworks for cybersecurity and CIIP, etc.

Resources (staff and budget): ITU/BDT/POL/CYB internal resources

Reference Material: ENISA (“Guide on how to set up a CERT”), Carnegie Mellon University, FIRST and CERT/CC resources (“Steps for Creating National CSIRTs”), GOVCERT.nl resources (“CSIRT in a Box”)

Related ITU Plenipotentiary Conference and/or WTDC-06 Mandate: Res. 130 (Rev. Antalya, 2006)

Related BDT Operational Plan Action Line(s): 9820 (2008), 9845 (2009)

8.2. Inventory of Watch, Warning and Incident Response Capabilities by Region

Objective: To review current activities worldwide and provide examples for developing countries who are establishing Watch, Warning and Incident Response Capabilities.

Activity Description: Conduct an inventory of CSIRT/CERT/etc. activities in the different countries on a regional basis. Compiled information to be distributed through a dedicated website and in a publication/CD-ROM.

Deliverables: Report with country information on CSIRT/CERT/etc. activities in the different countries, best practices, to be shared with the Member States through a dedicated website and publication/CD-ROM.

Partners: FIRST, ENISA, Carnegie Mellon University Software Engineering Institute, CERT/CC etc.

Priority: Medium

Deadlines: January 2008 for preliminary report on CSIRT activities in one region, ongoing for other regions

Promotion and Events: Regional workshops/forums on frameworks for cybersecurity and CIIP 2007, 2008, 2009.

Resources (staff and budget): ITU/BDT/POL/CYB internal resources

Reference Material: ENISA (detailed inventory of activities in Europe), CERT/CC and FIRST for overview of CERTs/CSIRTs

Related ITU Plenipotentiary Conference and/or WTDC-06 Mandate: Res. 130 (Rev. Antalya, 2006)

Related BDT Operational Plan Action Line(s): 10052 (2007), 9810 (2008)

8.3. CSIRT Toolkit

Objective: Provide countries with a practical toolkit that can assist in the establishment of national CSIRTs and enhance countries’ watch, warning and incident response (WWIR) capabilities

Activity Description: The CSIRT Toolkit provides a best practices/framework document containing the necessary elements and resources to establish a national watch, warning and incident response capability.

Deliverables: Toolkit to assist countries in the establishment of national CSIRTs

Partners: CERT/CC

Priority: Medium

Deadlines: December 2008

Promotion and Events: Regional workshops/forums on frameworks for cybersecurity and CIIP 2007, 2008, 2009.

Resources (staff and budget): ITU/BDT/POL/CYB internal resources

Reference Material: To be added

Related ITU Plenipotentiary Conference and/or WTDC-06 Mandate: Res. 130 (Rev. Antalya, 2006)

Related BDT Operational Plan Action Line(s): 10158 (2008)

8.4. Standard Reporting Format for Fraudulent Online Activities

Objective: Ensure that a standard reporting format for fraudulent online activities is available for all ITU Member States.

Activity Description: Creation and dissemination of a standard format for reporting fraudulent online activities in all ITU Member States. This would likely be based on the Anti-Phishing Working Group (APWG) and Internet Engineering Task Force (IETF) activities using the Incident Object Description Exchange Format (IODEF) XML Schema with possible e-crime relevant extensions. Under this scenario, using a common machine-readable XML reporting format, an Asian CSIRT could report a phishing incident to a European bank.

Deliverables: Standard reporting format for fraudulent online activities.

Partners: Anti-Phishing Working Group (APWG), IETF, ITU-T Study Group 17 and other relevant partners.

Priority: Low

Deadlines: End 2009

Promotion and Events: TBD

Resources (staff and budget): ITU/BDT/POL/CYB internal resources

Reference Material: To be added

Related ITU Plenipotentiary Conference and/or WTDC-06 Mandate: Res. 130 (Rev. Antalya, 2006)

Related BDT Operational Plan Action Line(s): 9817 (Unfunded) 2008

9. Countering Spam and Related Threats

Background Information: Spam is the abuse of messaging systems to send unsolicited bulk messages. While the most widely recognized form of spam is email spam, the term can also be applied to similar abuses in other media including instant messaging spam, Usenet newsgroup spam, Web search engine spam, spam in blogs, mobile messaging spam, Internet forum spam and junk fax transmissions. Spam is economically viable because advertisers have little or no operating costs beyond the management of mailing lists and it is difficult to identify and/or hold senders accountable for mass mailings. Because the barrier to entry is so low, spammers are numerous, and the volume of unsolicited mail has become very high – representing approximately 90% of all email. The costs, such as lost productivity and fraud, are borne by the end users and by Internet service providers, who have been forced to add extra capacity and spam blocking specialists to cope with the deluge. Spam is particularly problematic for developing countries that 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 which are used, for example, to construct botnets (see Section 9.2).

9.1. ITU Survey on Anti-Spam Legislation Worldwide

Objective: Share details of the current situation on anti-spam legislation in ITU Member States.

Activity Description: In 2005, ITU produced a survey of spam related legislation which needs to be updated with significant new legislative activity and analysis of what concrete actions countries are taking to deal with the growing problem of spam. An updated version of the ITU Survey on Anti-Spam Legislation Worldwide includes an examination of the anti-spam related activities in ITU’s 191 Member States based on survey responses, and a list of best practices in the area of anti-spam measures. The purpose of the survey is to better understand the approaches taken in the different regions and respective countries to fight spam and its related menaces. The results of the survey aims to help in understanding how risks related to spam are evaluated and managed by different countries, and also looks further into how specific development in the various sectors (e.g. telecommunication, financial sector, etc) and company types (e.g. multinational organizations, large companies, SMEs) has implemented changes to the legislation, as well as other approaches and activities. This aims to facilitate the communication between stakeholders in exchanging information about the methodologies and best practices in use presently. In conjunction with the release of an ITU anti-spam survey, a new set of spam-related web pages with up to date information on what activities ITU Member States are undertaking will be published.

Deliverables: Delivery of the 2007 ITU Survey on Anti-Spam Legislation Worldwide

Partners: StopSpamAlliance, Spamhaus, ITU-D RME, Messaging Anti-Abuse Working Group (MAAWG)

Priority: Medium

Deadlines: April 2008

Promotion and Events: TBD

Resources (staff and budget): ITU/BDT/POL/CYB internal resources

Reference Material: 2005 ITU Survey on Anti-Spam Legislation Worldwide, ITU spam resource sites, gathered material from Member States on updates to Member States' spam legislation gathered through the annual BDT survey (BDT Programme 1 activity)

Related ITU Plenipotentiary Conference and/or WTDC-06 Mandate: Res. 130 (Rev. Antalya, 2006)

Related BDT Operational Plan Action Line(s): TBD

9.2. Botnet Mitigation Toolkit

Objective: Provide a practical tool to help identify and take down botnets, and to raise awareness among Member States of the growing threats posed by botnets.

Activity Description: 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" – computers that can be controlled without the owners' knowledge. Criminals can use the collective computing power and connected bandwidth of these externally-controlled networks for malicious purposes and criminal activities, including, *inter alia*, generation of spam e-mails, launching of Distributed Denial of Service (DDoS) attacks, alteration or destruction of data, and identity theft. The threat from botnets is growing fast. The latest (2007) generation of botnets such as Zhelatin (Storm Worm) uses particularly aggressive techniques such as fast-flux networks and striking back with DDoS attacks against security vendors trying to mitigate them. An underground economy has now sprung up around botnets, yielding significant revenues for authors of computer viruses, botnet controllers and criminals who commission this illegal activity by renting botnets.

The botnet problem, like the spam problem, is even more acute in developing economies, due to:

- *Technical reasons* - expensive, restricted supply of bandwidth; lack of access to secure ICTs; ISP and network provider capacity issues in security awareness, etc.
- *Social reasons* - users are unfamiliar with the internet, vulnerable to viruses, scams; widespread use of pirated and insecure software and operating systems, etc.
- *Policy reasons* - lack of effective anti-spam and cybercrime laws and regulation; law enforcement and judiciary unfamiliar with computer crime issues; lack of international cooperation, engaging developing economies, etc.

Many of the issues described above are identical to the issues highlighted in earlier works on spam and malware, such as the OECD Antispam Toolkit and the ongoing APEC-TEL/OECD work on malware. Other country level initiatives include Australia’s Internet Security Initiative (AISI) which represents an innovative approach to mitigating botnets through cooperation with Internet Service Providers. The toolkit draws on existing resources, identifies relevant local and international stakeholders, and takes into consideration the specific constraints of developing economies.

Deliverables: A generic botnet mitigation toolkit that provides Member States with:

- Guidance on reliable, effective and evolving information sources of botnets scanning and detection;
- Model of government agency that coordinates the whole botnets mitigation activities from the detection to takedown;
- Framework of botnet-related regulation and enforcement;
- Environment to stress self-regulation of ISPs and raise of public security awareness;
- Guidance regarding mechanism for regional and international cooperation.

Priority: High

Partners: External consultant, ACMA, StopSpamAlliance partners, etc.

Deadlines: First draft of the toolkit background available in December 2007, with pilot tests planned in several Member States/regions in 2008/2009.

Promotion and Events: Website for launch of toolkit, CD-ROMs for all Member States and interested Sector Members/Associates, and other interested stakeholder. Toolkit CD-ROMs to be made available at all BDT and TSB events related to cybersecurity.

Resources (staff and budget): ITU/BDT/POL/CYB internal resources

Reference Material: Existing resources to be shared through a dedicated botnet webpage at http://www.itu.int/ITU-D/cyb/cybersecurity/projects/botnet.html

Related ITU Plenipotentiary Conference and/or WTDC-06 Mandate: Res. 130 (Rev. Antalya, 2006)

Related BDT Operational Plan Action Line(s): 9958 (2007), 9825 (2008), 9848 (2009)

9.3. Pilot Projects for Implementation of Botnet Mitigation Toolkit in ITU Member States

Objective: Providing developing countries with assistance in building capacity to identify and take down botnets.

Activity Description: Based on the botnet mitigation toolkit developed in Section 9.2, appropriate countries are identified for a small number of pilot projects to test the usefulness of the toolkit and refine it as appropriate. Relevant public and private stakeholders from the economy in question are approached to assist in the mitigation of botnets in their country. Relevant international stakeholders are also approached for their cooperation, where and when necessary.

Priority: High

Partners: External consultant, ACMA, StopSpamAlliance partners, etc.

Deadlines: Ongoing 2008 and 2009

Promotion and Events: Regional workshops/forums on frameworks for cybersecurity and CIIP 2007, 2008, 2009, and other relevant fora.

Resources (staff and budget): ITU/BDT/POL/CYB internal resources

Reference Material: Existing resources to be shared through a dedicated botnet webpage, http://www.itu.int/itu-d/cyb/cybersecurity/projects/botnet.html.

Related ITU Plenipotentiary Conference and/or WTDC-06 Mandate: TBD

Related BDT Operational Plan Action Line(s): 9825 (2008), 9848 (2009)

9.4. Joint Activities with StopSpamAlliance

Objective: Develop targeted assistance to developing countries on anti-spam measures.

Activity Description: The StopSpamAlliance is a joint initiative to gather information and resources on combating spam. This initiative was undertaken by APEC, the EU's CNSA, ITU, the London Action Plan, OECD and the Seoul-Melbourne Anti-Spam group. The partners have established a joint website at http://www.stopspamalliance.org, which is currently managed by the ITU. Members of the StopSpamAlliance would like to initiate targeted assistance to developing countries on anti-spam measures.

Deliverables: 2008 and 2009 deliverables to be defined together with StopSpamAlliance partners

Partners: StopSpamAlliance founding members and new associate partners (see http://www.stopspamalliance.org for reference to all involved partners).

Priority: Medium

Deadlines: Ongoing 2007, 2008, 2009

Promotion and Events: Regional workshops/forums on frameworks for cybersecurity and CIIP 2007, 2008, 2009.

Resources (staff and budget): ITU/BDT/POL/CYB internal resources

Reference Material: TBD

Related ITU Plenipotentiary Conference and/or WTDC-06 Mandate: Res. 130 (Rev. Antalya, 2006)

Related BDT Operational Plan Action Line(s): TBD

9.5. Study on Economics of Spam (with ITU-T Study Group 3)

Objective: Help Member States develop a better understanding of the economic aspects of spam in order to drive the right preventive activities in the country.

Activity Description: Threats to network security engender costs, either in the form of losses when security is breached, or in the form of protective measures to prevent breaches. An important element of network security costs is related to dealing with malware and spam. While malware and spam may have negative effects in the aggregate, individual stakeholders are affected in very different ways. They experience costs and benefits in different ways, leading to very different responses to the threats. To better understand the implications, an expert scoping study on the economics of malware and spam is conducted in cooperation with ITU-T Study Group 3 (working on tariff and accounting principles including related telecommunication economic and policy issues) and the ITU-D Regulatory and Market Environment Division (RME), responsible for Programme 4.

Deliverables: A background study on the economics of malware and spam will be shared with Member States in the first half of 2008.

Partners: ITU-D Programme 4, ITU-T Study Group 3, external consultant

Priority: Medium

Deadlines: June 2008

Promotion and Events: Deliverables to be shared at regional workshops/forums on frameworks for cybersecurity and CIIP in 2008 and 2009, and other relevant TSB and BDT fora.

Resources (staff and budget): ITU/BDT/POL/CYB internal resources, TSB resources, external experts

Reference Material: TBD

Related ITU Plenipotentiary Conference and/or WTDC-06 Mandate: Res. 130 (Rev. Antalya, 2006)

Related BDT Operational Plan Action Line(s): 9167 (2007)

9.6. Translation of Message Anti-Abuse Working Group Best Practices Documents

Objective: Make anti-spam/malware guides and reference materials developed by the Message Anti-Abuse Working Group available to ITU Member States into all six ITU/U.N. official languages

Activity Description: Translate reference materials developed by the Message Anti-Abuse Working Group into all six ITU/U.N. official languages. The first set of documents to be translated and made available to Member States include:

- MAAWG - Code of Conduct at http://www.maawg.org/about/CodeofConduct.pdf;
- MAAWG - Managing Port25 at http://www.maawg.org/port25;
- BIAC-MAAWG Best Practices Expansion Document at http://www.maawg.org/about/publishedDocuments/MAAWG-BIAC_Expansion0707.pdf;
- Anti-Phishing Best Practices for ISPs and Mailbox Providers at http://www.maawg.org/about/publishedDocuments/MAAWG_AWPG_Anti_Phishing_Best_Practices.pdf;
- MAAWG Sender BCP Version 1.1 at http://www.maawg.org/about/MAAWG_Sender_BCP, Executive Summary at http://www.maawg.org/about/MAAWG_Sender_BCP/MAAWGSendersBCP_ES.pdf.

Deliverables: Provide translated versions of the reference guides and material to the Member States through the BDT website and other appropriate channels.

Partners: Message Anti-Abuse Working Group (MAAWG)

Priority: Medium

Deadlines: January 2008

Promotion and Events: ITU website

Resources (staff and budget): ITU/BDT/POL/CYB internal resources, external experts

Reference Material: See websites referenced above.

Related ITU Plenipotentiary Conference and/or WTDC-06 Mandate: Res. 130 (Rev. Antalya, 2006)

Related BDT Operational Plan Action Line(s): TBD

9.7. Guide for Securing PCs, Applications, Mobile Phones, etc.

Objective: Increase Member States understanding of the need for protecting their citizens against threats caused by unprotected personal computers, applications, mobile phones, etc.

Activity Description: Creation of step-by-step user guidelines on how to make PCs, mobile phones and applications more secure and describing why security is important for end-users.

Deliverables: Guidelines for securing PCs, applications, mobile phones, etc.

Partners: TBD

Priority: Medium

Deadlines: December 2009

Promotion and Events: TBD

Resources (staff and budget): ITU/BDT/POL/CYB internal resources, external experts

Reference Material: TBD

Related ITU Plenipotentiary Conference and/or WTDC-06 Mandate: Res. 130 (Rev. Antalya, 2006)

Related BDT Operational Plan Action Line(s): 9841 (2009)

10. Bridging the Security-Related Standardization Gap

Background Information: ITU-T Study Group 17 is the Lead Study Group (LSG) for telecommunication security activities for the study period 2005-2008. This effort is carried out through Question 4/17 in close cooperation with other Study Groups in an effort to identify and develop security solutions. ITU-T SG 17 produces materials for developing countries that can be useful in identifying practical security solutions, such as the *ICT Security Standards Roadmap*. This online tool is now publicly-accessible at http://www.itu.int/ITU-T/studygroups/com17/ict/index.html and captures network-related security work of not only ITU-T but also of ISO/IEC, IETF, European Network and Information Security Agency (ENISA), the Network and Information Security Steering Group (NISSG), and consortia groups as part of their out-reach activities. ITU-T SG 17 produces additional materials useful for developing countries including, *inter alia*:

- A website on telecommunication security at http://www.itu.int/ITU-T/studygroups/com17/tel-security.html
- A Security Compendium including a “Catalogue of approved ITU-T Recommendations related to telecommunication security” available at http://www.itu.int/dms_pub/itu-t/oth/0A/0D/T0A0D0000090001MSWE.doc and an “Extract of ITU-T approved security definitions” available at http://www.itu.int/ITU-T/studygroups/com17/tel-security.html
- Summaries of all SG 17 Recommendations under development or revision. The latest draft summaries can be found at http://www.itu.int/ITU-T/studygroups/com17/SG 17final-summaries.doc
- Information summarizing ITU-T security-related activities. The information is available at http://www.itu.int/dms_pub/itu-t/oth/0A/0D/T0A0D0000050001MSWE.doc

Relevant World Telecommunication Standardization Assembly (WTSA) Resolutions include:

- Resolution 50: Cybersecurity (Florianopolis, 2004) at http://www.itu.int/ITU-T/wtsa/resolutions04/Res50E.pdf (see page 84)
- Resolution 51: Combating spam (Florianopolis, 2004) at http://www.itu.int/ITU-T/wtsa/resolutions04/Res51E.pdf (see page 85)
- Resolution 52: Countering spam by technical means (Florianopolis, 2004) at http://www.itu.int/ITU-T/wtsa/resolutions04/Res52E.pdf (see page 87)

10.1. Joint ITU-D/ITU-T Promotion of ITU-T Study Group 17 Activities

Objective: Deliver joint ITU-D/ITU-T promotion of ITU-T Study Group 17 security activities

Activity Description: Joint ITU-D/ITU-T promotion of ITU-T Study Group 17 security activities through different events and publications.

Deliverables: Joint ITU-D/ITU-T promotion of ITU-T Study Group 17 security activities

Partners: ITU-T SG17 and other relevant entities in the TSB

Priority: High

Deadlines: Ongoing 2007, 2008, 2009

Promotion and Events: Joint ITU-D/ITU-T events, regional workshops/forums on frameworks for cybersecurity and CIIP 2007, 2008, 2009.

Resources (staff and budget): ITU/BDT/POL/CYB internal resources

Reference Material: ITU event websites, http://www.itu.int/ITU-T/gap/

Related ITU Plenipotentiary Conference and/or WTDC-06 Mandate: Res. 130 (Rev. Antalya, 2006); Res. 123 (Rev. Antalya, 2006)

Related BDT Operational Plan Action Line(s): 9765 (Unfunded) (2008), and indirectly 2007 workshop related actions: 9031, 9718, 9757; 2008 workshop related actions: 9815, 9904, 9939, 10039, 10179; and 2009 actions 9941, 10041 (Unfunded), 10170

10.2. Increased Deployment and Awareness in Developing Countries of ITU-T Security-Related Standards

Objective: To distribute existing ITU-T security standards widely to ITU Member States and ensure that a larger number of participants from developing countries are involved in ITU's security standards development

Activity Description: Ensure that existing ITU-T security standards are distributed widely to ITU Member States, especially developing countries and least developed countries (LDCs), and ensure that a larger number of participants from developing countries are involved in ITU's security standards development. This also involves ensuring that the relevant material is translated, and specific text dedicated to developing country challenges in deploying security standards in existing TSB security-related standards is included.

Deliverables: Wide distribution of TSB security standards publications, roadmaps, texts. Ensuring that existing TSB security-related standards publication are translated and include reference to the specific challenges faced by developing countries.

Partners: ITU-T SG17 and other relevant entities in the TSB

Priority: Medium

Deadlines: Ongoing 2007, 2008, 2009

Promotion and Events: Joint ITU-D/ITU-T events, regional workshops/forums on frameworks for cybersecurity and CIIP 2007, 2008, 2009.

Resources (staff and budget): ITU/BDT/POL/CYB internal resources

Reference Material: http://www.itu.int/ITU-T/gap/

Related ITU Plenipotentiary Conference and/or WTDC-06 Mandate: Res. 130 (Rev. Antalya, 2006), Res. 123 (Rev. Antalya, 2006)

Related BDT Operational Plan Action Line(s): 9765 (Unfunded)(2008), and indirectly 2007 workshop related actions: 9031, 9718, 9757; 2008 workshop related actions: 9815, 9904, 9939, 10039, 10179; and 2009 actions 9941, 10041 (Unfunded), 10170

11. Project on Enhancing Cybersecurity and Combating Spam

Background information: Resolution 130 (Rev. Antalya, 2006) instructs the Director of the Telecommunication Development Bureau:

1. to develop, consistent with the results of WTDC-06 and the subsequent meeting pursuant to Resolution 45 (Doha, 2006) of that conference, the projects for enhancing cooperation on cybersecurity and combating spam responding to the needs of developing countries, in close collaboration with the relevant partners;

2. to provide the necessary financial and administrative support for these projects within existing resources, and to seek additional resources (in cash and in kind) for the implementation of these projects through partnership agreements;

3. to ensure coordination of these projects within the context of ITU's overall activities in its role as moderator/facilitator for WSIS action line C5;

4. to coordinate these projects with the activities and programmes of ITU-D study groups on this topic;

5. to continue collaboration with relevant organizations with a view to exchanging best practices and disseminating information through, for example, joint workshops/forums and training sessions;

11.1. Formulation of Project on Enhancing Cybersecurity and Combating Spam

Objective: Ensure delivered activities in all areas mentioned in the report from meeting held subsequently to the WTDC 2006 Resolution 45 cybersecurity project and referenced in ITU Plenipotentiary *Resolution 130 (Rev. Antalya, 2006): Strengthening the role of ITU in building confidence and security in the use of information and communication technologies*.

Activity Description: Creation of a project document to ensure that all activities referenced in the WTDC 2006 Resolution 45 cybersecurity project "Project on Enhancing Cybersecurity and Combating Spam" are being considered by the BDT. Resolution 130 (Rev. Antalya, 2006) instructs the BDT director to develop the projects "responding to the needs of developing countries, in close collaboration with the relevant partners".

Deliverables: Cybersecurity project document with details on ongoing and planned projects related to the Resolution 45 (Doha, 2006) cybersecurity project: "*ITU Cybersecurity Work Programme for Developing Countries*"

Partners: Internal ITU

Priority: High

Deadlines: First draft of the *ITU Cybersecurity Work Programme for Developing Countries* was released in June 2007, with a revised version released in December 2007. Ongoing revisions to be made throughout 2008 and 2009.

Promotion and Events: All cybersecurity-related events

Resources (staff and budget): ITU/BDT/POL/CYB internal resources

Reference Material: Resolution 130 (Antalya, 2006), Resolution 45 (Doha, 2006), Report from the workshop called for by Resolution 45 (draft project document 2006 version).

Related ITU Plenipotentiary Conference and/or WTDC-06 Mandate: Res. 130 (Rev. Antalya, 2006), Resolution 45 (Doha, 2006)

Related BDT Operational Plan Action Line(s): N/A

12. Cybersecurity Indicators

Background Information: There are a lack of indicators that can be used by countries to benchmark and/or measure progress in building confidence and security in the use of ICTs.

12.1. Elaboration and Development of Indicators for Cybersecurity

Objective: Develop a common approach for benchmarking cybersecurity to assist countries in measuring, assessing and re-assess cybersecurity readiness, particularly against other countries at the same level of socio-economic development.

Activity Description: As cybersecurity is one of the key priorities for Programme 3, one important requirement is to benchmark different elements of cybersecurity (e.g. spam, viruses, phishing) to gain an insight into the reliability of today's ICT networks and the challenges they face (and ultimately whether any progress is being made in building confidence and security in the use of ICTs). This benchmarking can then be used for a more detailed analysis of cybersecurity trends, both at the level of geography (national, regional, and international) and in terms of the different threats. Developing a common set of metrics for cybersecurity involves a number of different agencies and organizations, and requires a combination of commissioned studies, desk research and a series of meetings/workshops/forums.

Deliverables: Development of toolkit with a common set of metrics for cybersecurity

Partners: BDT Market Information and Statistics Unit (STAT), Partnership on Measuring ICT for Development, external partners, external consultant

Priority: Medium

Deadlines: December 2008

Promotion and Events: TBD

Resources (staff and budget): ITU/BDT/POL/CYB internal resources

Reference Material: TBD

Related ITU Plenipotentiary Conference and/or WTDC-06 Mandate: Res. 130 (Rev. Antalya, 2006)

Related BDT Operational Plan Action Line(s): 9827 (2008)

13. Fostering Regional Cooperation Activities

Background Information: To leverage activities such as awareness and capacity building, the national cybersecurity/CIIP self-assessment toolkit and other activities/resources of the ICT Applications and Cybersecurity Division, regional cooperation activities need to be fostered and established to build cooperation networks among countries to share expertise and experiences.

13.1. Assistance in Establishment of Regional Cooperation Activities of National Cybersecurity/CIIP Actors

Objective: Provide assistance to ITU Member States in establishing regional cooperation activities of national cybersecurity/critical information infrastructure protection (CIIP) actors.

Activity Description: Ongoing assistance to ITU Member States in establishing regional cooperation activities of national cybersecurity/critical information infrastructure protection (CIIP) actors.

Deliverables: TBD

Partners: ITU Member States

Priority: High

Deadlines: Ongoing 2007, 2008, 2009

Promotion and Events: Regional cybersecurity events organized by BDT and TSB, WSIS Action Line C5 related events

Resources (staff and budget): ITU/BDT/POL/CYB internal resources

Reference Material: TBD

Related ITU Plenipotentiary Conference and/or WTDC-06 Mandate: Res. 130 (Rev. Antalya, 2006)

Related BDT Operational Plan Action Line(s): TBD

14. Information Sharing and Supporting the ITU Cybersecurity Gateway

Background information: ITU Plenipotentiary Resolution 130 (Rev. Antalya, 2006) requires a review of the work done to date by ITU and other relevant organizations, and their initiatives to address existing and future threats in order to build confidence and security in the use of ICTs. In order for ITU to play an important role in the area of cybersecurity globally, assisting Member States and fostering information exchange and cooperation between related actors, the organization needs to establish a directory of relevant organizations with contact information for both internal and external coordination purposes along with different levels of access control to contact points. In addition, based on information that can be made public, ITU will publish an annual Directory of Who's Who in Cybersecurity/CIIP which can serve as reference material for regional and international cooperation initiatives.

14.1. Establishment of an ITU Cybersecurity/CIIP Directory

Objective: Gather and maintain information on organizations/entities active in the different areas of cybersecurity worldwide. Ensure that ITU globally provides the main platform for this kind of information.

Activity Description: The establishment of an ITU Cybersecurity/CIIP Directory is necessary to provide a comprehensive listing of organizations that work and have activities in the area of cybersecurity/CIIP (see *Annex C: Organisations Involved in Cybersecurity Initiatives* on page 89). Entries in the Directory are categorized by location, organization type, specific activity area and responsibilities, and have associated contact details, links to the organization's website, and a short description of the organization's activities.

The Directory gives all interested parties one single place/publication/website access to contact data and entry points for a multitude of contacts worldwide. The Directory provides information on national leaders in all ITU Member States as well as information on regional institutions and international bodies active in cybersecurity. The Cybersecurity Directory can build on information already available in the SQL databases currently behind the ITU Cybersecurity Gateway and the planned internal ITU Cybersecurity Contact Database (see Activity 14.2). In order to expand on the information available in the Cybersecurity Gateway, ITU Member States and the international community need to continue to cooperate and provide ITU with the relevant data. The Directory requires constant updating in order to remain current and valuable for all the different parties interested in Network and Information Security. Consideration needs to be given as what linkages this Directory would have with information in the ITU Global Directory and ICT Eye and the web-based graphical presentation format.

Deliverables: ITU cybersecurity/CIIP directory of actors with responsibilities and contact details

Partners: TBD

Priority: Medium

Deadlines: Ongoing 2007, 2008, 2009

Promotion and Events: TBD

Resources (staff and budget): ITU/BDT/POL/CYB internal resources

Reference Material: ITU Cybersecurity Gateway, ITU ICT eye

Related ITU Plenipotentiary Conference and/or WTDC-06 Mandate: Res. 130 (Rev. Antalya, 2006)

Related BDT Operational Plan Action Line(s): 9823 (2008), 9839 (2009)

14.2. Establishment of an ITU Cybersecurity/CIIP Contact Database

Objective: To share the cybersecurity contact information through an online tool, internally and with appointed country representatives, and selected experts from partner organizations.

Activity Description: To make accessible the valuable information obtained in the contact directory (14.1), there is a need for a cybersecurity contact database that allows for information to be shared electronically. As it is essential for ITU to establish, maintain and develop relationships with and between other international bodies active in the different areas of security, with Member State initiatives and their specific focal points, a single database for this information is key. The ITU cybersecurity contact database could be developed and implemented based on the work already done and code in place for the ITU Cybersecurity Gateway and/or ICT Eye. Additional development, however, is required and the contacts database should be made accessible through a common web interface and with different levels of authenticated access.

Viewable fields: ITU users would be able to pull information from the following fields pertaining to a contact including: Region, Country, Type of Organization (Government International Organization Business Non-Governmental Organization Partnership Other), Name of Organization/Institution, Main Contact (Last name First name), Position/Title, Address, City and/or Postal code, Telephone, Fax, E-mail, Website, Areas of interest, Other information/ Description

Search functionality: internal and external users should be able to search the contacts database by matching a query on specific fields (e.g., country). Add/edit/delete functionality is required so that external designated entities can update their associated contact information. The contact database needs to be SQL based, to ensure not only easy access to the information, but also to make future integration into other web-based tools possible (i.e. Cybersecurity Gateway, ICT Eye, etc.). Consideration also needs to be made of mechanisms to support different levels of trust among cybersecurity actors (e.g., government only).

Deliverables: Cybersecurity contact database and processes for maintaining and updating the information in the database.

Partners: TBD

Priority: Medium

Deadlines: Q2 2008 but ongoing activities and resources required

Promotion and Events: TBD

Resources (staff and budget): ITU/BDT/POL/CYB internal resources

Reference Material: ITU Cybersecurity Gateway, ITU survey results, ENISA Who's Who Directory for EU countries, etc.

Related ITU Plenipotentiary Conference and/or WTDC-06 Mandate: Res. 130 (Rev. Antalya, 2006)

Related BDT Operational Plan Action Line(s): 9823 (2008), 9839 (2009)

14.3. Establishment of Annual Who's Who in Cybersecurity/CIIP Publication

Objective: Encourage Member States and relevant cybersecurity stakeholders to share their information through an ITU platform.

Activity Description: Annual publication/CD-ROM based on information gathered in Sections 14.1 and 14.2 explained above. This information could be distributed to the Membership and other stakeholder in a number of ways; annual ITU Cybersecurity Publication, sent out to Member States free of charge in an effort to remind them to send us up to date information on the main stakeholders in the respective countries.

Deliverables: Publication/CD-ROM with the main actors in Cybersecurity in all 191 ITU Member States

Partners: TBD

Priority: Medium

Deadlines: Ongoing 2008, 2009

Promotion and Events: TBD

Resources (staff and budget): ITU/BDT/POL/CYB internal resources

Reference Material: Information available in the ITU Cybersecurity Gateway, ITU survey results, ENISA Who's Who directory for EU countries, etc.

Related ITU Plenipotentiary Conference and/or WTDC-06 Mandate: Res. 130 (Rev. Antalya, 2006)

Related BDT Operational Plan Action Line(s): 9823 (2008), 9839 (2009)

14.4. Establishment of an Annual ITU Cybersecurity Publication

Objective: This annual cybersecurity flagship publication shares information on what is happening in the areas related to Cybersecurity and countering spam, and provides an analysis of the current environment, main trends and progress made in the Member States and activities of the different stakeholders.

Activity Description: The ITU Cybersecurity Publication is a key product to provide an overview of what is happening in Member States with regards to cybersecurity and countering spam.

Deliverables: Annual ITU cybersecurity publication

Partners: ITU Sectors and interested parties, Member States, Sector Members/Associates and external experts

Priority: Medium

Deadlines: Q3 2008 launch of first publication, Q3 2009 launch of second publication

Promotion and Events: Main ITU events and specific ITU workshops/forums related to cybersecurity

Resources (staff and budget): ITU/BDT/POL/CYB internal resources

Reference Material: ITU Cybersecurity Gateway, blog material, news articles and work/analysis done in the ITU-D Study Group Q 22/1, and other ITU study groups and interest groups, etc.,

Related ITU Plenipotentiary Conference and/or WTDC-06 Mandate: Res. 130 (Rev. Antalya, 2006)

Related BDT Operational Plan Action Line(s): 9814 (2008), 9837 (2009)

14.5. ITU Cybersecurity Fellowship Programme for Developing Countries

Objective: Increase awareness and give young people from developing countries exposure to the main issues related to cybersecurity, and to the ongoing work of ITU in this domain.

Activity Description: Develop an ITU cybersecurity fellowship programme for participants from developing countries. The purpose of the initiative is to increase awareness on issues related to cybersecurity (mainly amongst young people and students), and to the ongoing work of ITU in this domain, through an essay writing competition and dedicated ITU cybersecurity fellowship programme. The fellowships granted aims to help build capacity in developing countries as the competition winners attend ITU cybersecurity/CIIP related events, conduct research activities and engage in specific

ITU cybersecurity related activities for the duration of the programme. The selected applicants have the opportunity to have their work posted on the ITU website and/or cited in an ITU-D publication. In addition, the cybersecurity essay competition winners are offered the opportunity of a short-term research contract with the ICT Applications and Cybersecurity Division for three months, and a contribution to the cost of an economy class flight from their current place of residence, plus CHF 10'000 towards living expenses while in Geneva.

Deliverables: Annual ITU essay competition and related fellowship programme with chosen fellows for 2008 and 2009

Partners: TBD

Priority: Medium

Deadlines: Activity to be launched in 2008 with the first competition with a continuation in 2009

Promotion and Events: Main ITU events and specific ITU workshops/forums related to cybersecurity

Resources (staff and budget): ITU/BDT/POL/CYB internal resources

Reference Material: General ITU Internship Programme on ITU website

Related ITU Plenipotentiary Conference and/or WTDC-06 Mandate: TBD

Related BDT Operational Plan Action Line(s): 9822 (2008), 9842 (2009)

14.6. Enhancement of the ITU Cybersecurity Gateway

Objective: To ensure that the ITU Cybersecurity Gateway is the main website for cybersecurity actors and relevant information on cybersecurity worldwide.

Activity Description: The ITU Cybersecurity Gateway (http://www.itu.int/cybersecurity/gateway/) is an in-house developed web portal and information sharing resource that generically supports all ongoing and planned ITU cybersecurity activities, both in the General Secretariat and Sectors. The databases behind the gateway are SQL-based. The following activities are proposed to be undertaken in 2007/2008 to improve the ITU Cybersecurity Gateway, particularly to enhance its resources to assist developing countries:

- Improve the structure of the ITU Cybersecurity Gateway in order to allow for static web pages in all six official ITU/UN languages;
- Translate the static pages of the portal into all six official ITU/UN languages and set up procedure for the translation of new material as it is added;
- Enhance the report running functionalities from the SQL databases (this would include the writing of new reports);
- Develop an online calendar for cybersecurity-related events worldwide;

- Set up of a parallel “internal” portal secured with login and password for sharing of critical information between the different interest groups to allow them to easily exchange information and good practices in a secure manner. This would include different levels of authentication for user communities. The relationship between this activity and the recently established ITU-D Q22/1 discussion forum would have to be clarified further.
- Set up of a dedicated cybersecurity blog within the portal. This blog could have one “open” area managed by ITU as well a blog area where selected security experts share their thoughts on topics of interest with the goal of enhancing the knowledge base of experts from developing countries;
- Ensure that the ITU Cybersecurity Gateway supports, where ever appropriate, all ITU cybersecurity-related activities;
- Set up of ITU mechanism for adding/removing/updating/changing links and material on the static Gateway pages and for the cybersecurity-related entries in the underlying database
- Expand the number of “topics” covered in the Gateway to ensure that the resources reflect the evolving cyber-threats;
- Create better links to other resources within and external to ITU (for example, ITU ICT Eye, training databases, etc.), and create linkages to ongoing and planned ITU-D related work programme activities;
- Provide new mapping interface for the Cybersecurity Gateway

Deliverables: An improved structure behind the ITU Cybersecurity Gateway and processes for updating and maintaining the Cybersecurity Gateway with relevant information on cybersecurity worldwide as well as ensuring that the Cybersecurity Gateway is used in an efficient manner to promote and support ITU activities in security. Integrate an improved mapping interface into the Cybersecurity Gateway based on information available in the underlying databases.

Partners: Internal ITU and external experts.

Priority: Medium

Deadlines: End 2008

Promotion and Events: Through ITU website and relevant publications/flyers/posters/articles

Resources (staff and budget): ITU/BDT/POL/CYB internal resources. Additional hardware may be required to support the needs of the expanding ITU Cybersecurity Gateway. A dedicated staff member would be responsible for constantly updating the current information as well as to increase the number of entries in the ITU Cybersecurity Gateway database to ensure that there is data available for the different stakeholders in all 191 ITU Member States.

Reference Material: ITU Cybersecurity Gateway at http://www.itu.int/cybersecurity/gateway/ and reference to ITU security-related activities at http://www.itu.int/cybersecurity/, ITU/BDT/POL/CYB web resources at http://www.itu.int/ITU-D/cyb/.

Related ITU Plenipotentiary Conference and/or WTDC-06 Mandate: Res. 130 (Rev. Antalya, 2006) references the Cybersecurity Gateway and instructs the Secretary-General and Directors of the Bureaux to ensure that the Cybersecurity Gateway is maintained and information displayed in the databases and static web pages is further extended.

Related BDT Operational Plan Action Line(s): 9816 (2008), 9838 (2009)

15. Outreach and Promotion

Overview: Other Promotion and Outreach of activities related to this *Cybersecurity Work Programme*.

15.1. Outreach and Promotion of Related Activities

Objective: Ensure that BDT cybersecurity and countering spam activities are effectively promoted through existing channels and synergies found with activities undertaken by BDT, TSB, BR, TELECOM and the General Secretariat.

Activity Description: While all components in the *Cybersecurity Work Programme to Assist Developing Countries* (2007-2009) have a “Promotion and Events” element, synergies also need to be assured with other related ITU activities. Close collaboration and information sharing is therefore needed on multiple levels, across the organization.

Deliverables: Related to other activities in this *Cybersecurity Work Programme*. Concrete activities will be developed.

Partners: BDT Partnerships and Promotion Unit (PPI), other entities in BDT, TSB, BR, TELECOM and the General Secretariat.

Priority: High

Deadlines: Ongoing 2007, 2008, 2009

Promotion and Events: Internet Governance Forum (IGF) meetings, major ITU events. Material created for and through the activities listed in the *Cybersecurity Work Programme*, including links to web pages, online toolkits, etc. to be shared with relevant parties in the ITU for further distribution.

Resources (staff and budget): ITU/BDT/POL/CYB internal resources

Reference Material: TBD

Related ITU Plenipotentiary Conference and/or WTDC-06 Mandate: Res. 130 (Rev. Antalya, 2006)

Related BDT Operational Plan Action Line(s): 9170 (2007)

Annex A: Overview of Detailed Initiatives

High Level Assistance Activity	Initiative Reference	Title of Initiative	Deliverables	Partners	Deadlines	Resources (staff and budget)	Priority
General Management and Coordination	4.1	General Management and Coordination	Efficient administration of Work Programme activities	TBD	N/A	TBD	N/A

High Level Assistance Activity	Initiative Reference	Title of Initiative	Deliverables	Partners	Deadlines	Resources (staff and budget)	Priority
ITU Member States' Cybersecurity Requirements and Mutual Assistance Capabilities	5.1	Review of ITU Member States' needs	1) Map ITU-D Study Group 22/1 framework activities against activities in this document. Develop a strategy to reach maximum number of Member States for awareness raising and targeted capacity building. 2) ITU National Cybersecurity/CIIP Self Assessment Toolkit 3) Establish list of key national cybersecurity contacts	ITU Member States, ITU Regional Offices	Ongoing assessment of Member States' needs in cybersecurity and countering spam 2007, 2008, 2009	9167 (2007), 9819, 10038 (2008), 9844 (2009)	High
National Strategies and Capabilities	6.1	Identification of Best Practices in the Establishment of National Frameworks for Cybersecurity and CIIP	Successful delivery of the ITU-D Study Group 1 Question 22 Report	ITU-D Study Group 1 Question 22, other relevant parties	Study Group 1 Question 22 has a four year study cycle (2006-2010)	9757(2007), 9819 (2008), 9844 (2009) and 10038 (2008)	High

High Level Assistance Activity	Initiative Reference	Title of Initiative	Deliverables	Partners	Deadlines	Resources (staff and budget)	Priority
National Strategies and Capabilities	6.2	Country Case Studies for Best Practices in the Establishment of National Frameworks for Cybersecurity and Critical Information Infrastructure Protection	Case studies	TBD	December 2008	Internal resources	Low
National Strategies and Capabilities	6.3	Regional Workshops/Forums on Frameworks for Cybersecurity and CIIP	Delivery of regional workshops/forums on frameworks for cybersecurity and critical information infrastructure protection.	Regional offices, relevant TSB parties, specific organizations with specific mandate and expertise, external experts	Ongoing 2007, 2008,2009	2007 workshop related actions: 9031, 9718, 9757, 10096; 2008 workshop related actions: 9815, 9904, 9939, 10039, 10179; 2009 workshop related actions 9941, 10041 (Unfunded), 10170	High
National Strategies and Capabilities	6.4	National Cybersecurity/CIIP Readiness Self-Assessment Toolkit	Toolkit and related training material for Member States	ITU-D Study Group 22/1, and other relevant entities, organizations, etc.	December 2007	9167(2007)	High

High Level Assistance Activity	Initiative Reference	Title of Initiative	Deliverables	Partners	Deadlines	Resources (staff and budget)	Priority
National Strategies and Capabilities	6.5	Pilot Projects in ITU Member States for Implementation of the National Cybersecurity/CIIP Readiness Self-Assessment Toolkit	Implementation of pilot projects in the Member States	ITU-D Study Group 22/1, and other relevant entities, organizations, etc.	First pilot project in Vietnam, August 2007, second pilot project in Argentina, October 2007, third pilot project in Ghana, November 2007. For 2008 and 2009, pilot self-assessments are planned for countries in Africa, Arab States, Asia Pacific, Americas, Europe/CIS	6167 (2007), 10038 (2008), 9844 (2009)	High
National Strategies and Capabilities	6.6	Online Cybersecurity Forum to Help Developing Countries Build Capacity	Implementation of an online cybersecurity forum	ITU-D Study Group 22/1, other relevant entities within ITU, external experts to help moderate the online forum	December 2008 for launch of forum	9764 (2008), 9843 (2009)	Medium

High Level Assistance Activity	Initiative Reference	Title of Initiative	Deliverables	Partners	Deadlines	Resources (staff and budget)	Priority
National Strategies and Capabilities	6.7	Toolkit for Promoting a Culture of Cybersecurity	Toolkit for promoting a culture of cybersecurity	ITU-D Study Group Q22/1, other entities within ITU, external experts	December 2009	9821, 9836 (2009)	Medium
National Strategies and Capabilities	6.8	Online Training Modules for Cybersecurity Awareness and Solutions	Delivery of online training modules for raising awareness on cybersecurity and CIIP	ITU Centers of Excellence, ITU-D Study Group 22/1, other relevant entities within ITU, and external experts and entities.	Ongoing 2008, 2009	9818 (2009)	Medium
Legislation and Enforcement Mechanisms	7.1	Regional Capacity Building Activities on Cybercrime Legislation and Enforcement	Regional and global workshops/forums, training material	Council of Europe, UNODC, other relevant regional and international organizations, national departments of justice	Ongoing 2007, 2008, 2009	2007 workshop related actions: 9031, 9718, 9757, 10096; 2008 workshop related actions: 9815, 9824 (Unfunded), 9904, 9939, 10039, 10179; and 2009 actions 9846 (Unfunded), 9941, 10041 (Unfunded), 10170	High

High Level Assistance Activity	Initiative Reference	Title of Initiative	Deliverables	Partners	Deadlines	Resources (staff and budget)	Priority
Legislation and Enforcement Mechanisms	7.2	Revision of Existing Cybersecurity Publication and Launch of Publication on Understanding Cybercrime	Revised publication, and one new publication	External expert with peer review by representatives from relevant international, regional, and national entities, including interested national departments of justice	Q1 2008	9167 (2007)	High
Legislation and Enforcement Mechanisms	7.3	Toolkit for Cybercrime Legislation for Developing Countries	Toolkit	Multidisciplinary and international group of experts	March 2008	9172 (2007), 9824 (Unfunded), 9826 (Unfunded) (2008), 9846 (Unfunded) (2009)	High
Legislation and Enforcement Mechanisms	7.4	Cybersecurity Module in the ITU/InfoDev ICT Regulation Toolkit	TBD	TBD	December 2009	9766 (Unfunded)(2008)	Medium

High Level Assistance Activity	Initiative Reference	Title of Initiative	Deliverables	Partners	Deadlines	Resources (staff and budget)	Priority
Watch, Warning and Incident Response (WWIR) Capabilities	8.1	Assistance to Developing Countries Related to Establishment of Watch, Warning and Incident Response (WWIR) Capabilities	Capacity building activities related to WWIR	FIRST, ENISA, CERT/CC, Carnegie Mellon University SEI, National/Regional CSIRTs	Ongoing 2008 and 2009	9820 (2008), 9845 (2009)	Medium
Watch, Warning and Incident Response (WWIR) Capabilities	8.2	Inventory of Watch, Warning and Incident Response Capabilities by Region	Report	FIRST, ENISA, Carnegie Mellon University SEI, CERT/CC.	January 2008 for preliminary report on CSIRT activities in one region, ongoing for other regions	10052 (2007), 9810 (2008)	Medium
Watch, Warning and Incident Response (WWIR) Capabilities	8.3	CSIRT Toolkit	CSIRT Toolkit	CERT/CC	December 2008	10158 (2008)	Medium
Watch, Warning and Incident Response (WWIR) Capabilities	8.4	Standard Reporting Format for Fraudulent Online Activities	Standard reporting format for fraudulent online activities	APWG and other relevant partners	End 2009	9817 (Unfunded) 2008	Low

High Level Assistance Activity	Initiative Reference	Title of Initiative	Deliverables	Partners	Deadlines	Resources (staff and budget)	Priority
Countering Spam and Related Threats	9.1	ITU Survey on Anti-Spam Legislation Worldwide	Report	TBD	February 2008	Internal resources	Medium
Countering Spam and Related Threats	9.2	Botnet Mitigation Toolkit	Toolkit	Expert	December 2007, pilot tests in 2008 and 2009	9958 (2007)	High
Countering Spam and Related Threats	9.3	Pilot Projects for Implementation of Botnet Mitigation Toolkit in ITU Member States	Pilot Projects	Expert	Ongoing 2008 and 2009	9825 (2008), 9848 (2009)	High
Countering Spam and Related Threats	9.4	Joint Activities with StopSpamAlliance	2008 and 2009 activities to be defined with StopSpamAlliance partners	StopSpamAlliance founding members and new associate partners	Ongoing 2007, 2008, 2009	TBD	Medium
Countering Spam and Related Threats	9.5	Study on Economics of Spam (with ITU-T Study Group 3)	Report	ITU-D Programme1, ITU-T Study Group 3, external consultant	January 2008	9167 (2007)	Medium

High Level Assistance Activity	Initiative Reference	Title of Initiative	Deliverables	Partners	Deadlines	Resources (staff and budget)	Priority
Countering Spam and Related Threats	9.6	Translation of Message Anti-Abuse Working Group Best Practices Documents	Translated documents	MAAWG	January 2008	Internal ITU	Medium
Countering Spam and Related Threats	9.7	Guide for Securing PCs, Applications, Mobile Phones, etc.	Guide for securing PCs, applications, mobile phones, etc	TBD	December 2009	9841 (2009)	Medium
Bridging the Security-Related Standardization Gap	10.1	Joint ITU-D/ITU-T Promotion of ITU-T Study Group 17 Activities	Joint ITU-D/ITU-T promotion of ITU-T Study Group 17 security activities	ITU-T SG17 and other relevant entities in the TSB	Ongoing 2007, 2008, 2009	9765 (Unfunded)(2008), and indirectly 2007 workshop related actions: 9031, 9718, 9757; 2008 workshop related actions: 9815, 9904, 9939, 10039, 10179; and 2009 actions 9941, 10041 (Unfunded), 10170	Medium

High Level Assistance Activity	Initiative Reference	Title of Initiative	Deliverables	Partners	Deadlines	Resources (staff and budget)	Priority
Bridging the Security-Related Standardization Gap	10.2	Increased Deployment and Awareness in Developing Countries of ITU-T Security-Related Standards	Wide distribution of TSB security standards publications, roadmaps, texts, etc.	ITU-T SG17 and other relevant entities in the TSB	Ongoing 2007, 2008, 2009	9765 (Unfunded)(2008), and indirectly 2007 workshop related actions: 9031, 9718, 9757; 2008 workshop related actions: 9815, 9904, 9939, 10039, 10179; and 2009 actions 9941, 10041 (Unfunded), 10170	Medium
Project on Enhancing Cybersecurity and Combating Spam	11.1	Formulation of Project on Enhancing Cybersecurity and Combating Spam	ITU Cybersecurity Work Programme for Developing Countries	Internal ITU	First draft released in June 2007, revised version in November 2007. Ongoing revisions 2008 and 2009	Internal ITU	High
Cybersecurity Indicators	12.1	Elaboration and Development of Indicators for Cybersecurity	Toolkit	BDT Market Information and Statistics Unit (STAT), external partners, external consultant	December 2008	9827 (2008)	Medium

High Level Assistance Activity	Initiative Reference	Title of Initiative	Deliverables	Partners	Deadlines	Resources (staff and budget)	Priority
Fostering Regional Cooperation Activities	13.1	Assistance in Establishment of Regional Cooperation Activities of National Cybersecurity/CIIP Actors	TBD	ITU Member States	Ongoing 2007, 2008, 2009	TBD	High
Information Sharing and Supporting the ITU Cybersecurity Gateway	14.1	Establishment of an ITU Cybersecurity/CIIP Directory	ITU cybersecurity/CIIP directory of actors with responsibilities and contact details	TBD	December 2008	Internal ITU staff	Medium
Information Sharing and Supporting the ITU Cybersecurity Gateway	14.2	Establishment of an ITU Cybersecurity/CIIP Contact Database	Cybersecurity contact database and processes for maintaining and updating the information in the database.	TBD	December 2008	Internal ITU staff	Medium
Information Sharing and Supporting the ITU Cybersecurity Gateway	14.3	Establishment of Annual Who's Who in Cybersecurity/CIIP Publication	Publication/CD-ROM with the main actors in Cybersecurity in all 191 ITU Member States	TBD	Ongoing 2008, 2009	9823 (2008), 9839 (2009)	Medium

High Level Assistance Activity	Initiative Reference	Title of Initiative	Deliverables	Partners	Deadlines	Resources (staff and budget)	Priority
Information Sharing and Supporting the ITU Cybersecurity Gateway	14.4	Establishment of an Annual ITU Cybersecurity Publication	Annual ITU cybersecurity publication	TBD	Q3 2008, Q3 2009	9814 (2008), 9837 (2009)	Medium
Information Sharing and Supporting the ITU Cybersecurity Gateway	14.5	ITU Cybersecurity Fellowship Programme for Developing Countries	Annual ITU essay competition and related fellowship programme with chosen fellows for 2008 and 2009	TBD	Launched in 2008 with the second competition in 2009	9822 (2008), 9842 (2009)	Medium
Information Sharing and Supporting the ITU Cybersecurity Gateway	14.6	Enhancement of the ITU Cybersecurity Gateway	Enhancement of the ITU Cybersecurity Gateway (databases, mapping interface)	TBD	Q2 2008	9816 (2008), 9838 (2009)	Medium
Outreach and Promotion	15.1	Outreach and Promotion of Related Activities	TBD	BDT Partnerships and Promotion Unit (PPI), other entities in BDT, TSB, BR, TELECOM and the General Secretariat	Ongoing 2007, 2008, 2009	9170 (2007)	High

Annex B: ITU Resolutions Relating to Cybersecurity

Resolution 130 (Rev. Antalya, 2006): Strengthening the role of ITU in building confidence and security in the use of information and communication technologies

The Plenipotentiary Conference of the International Telecommunication Union (Antalya, 2006),

considering

a) the crucial importance of information and communication infrastructures and their applications to practically all forms of social and economic activity;

b) that with the application and development of information and communication technologies (ICTs), new threats from various sources have emerged that may have an impact on confidence and security in the use of ICTs by all Member States, Sector Members and other stakeholders, including all users of ICT, and on the preservation of peace and the economic and social development of all Member States, and that threats to and vulnerabilities of networks continue to give rise to ever-growing security challenges across national borders for all countries, in particular developing countries, including least developed countries, small island developing states and countries with economies in transition, while noting in this context the need to further enhance international cooperation and develop and adapt appropriate existing national, regional and international mechanisms (for example agreements, best practices, memorandums of understanding, etc);

c) that, in order to protect these infrastructures and address these challenges and threats, coordinated national action is required for prevention, preparation, response and recovery from an incident on the part of government authorities at the national, state/provincial and local levels; the private sector, citizens and users, in addition to international cooperation and coordination,

recognizing

a) that the application and development of ICTs have been and continue to be instrumental for the growth and development of the global economy, underpinned by security and trust;

b) that the World Summit on the Information Society (WSIS) recognized the need to build confidence and security in the use of ICTs, the great importance of multi-stakeholder implementation at the international level and established Action Line C5, “Building confidence and security in the use of ICTs”, with ITU identified in the Tunis Agenda as moderator/facilitator for this WSIS Action Line;

c) that the World Telecommunication Development Conference (Doha, 2006) (WTDC) has adopted the Doha Action Plan and its programme 3 on e-strategies and ICT applications that identifies cybersecurity as a priority activity of BDT and defines activities to be undertaken by BDT, and in particular the adoption of Resolution 45 (Doha, 2006) entitled “Mechanisms for enhancing cooperation on cybersecurity, including combating spam”;

d) § 15 of the Tunis Commitment which recognizes “the principles of universal and non-discriminatory access to ICTs for all nations, the need to take into account the level of social and economic development of each country, and respecting the development-oriented aspects of the Information Society, we underscore that ICTs are effective tools to promote peace, security and stability, to enhance democracy, social cohesion, good governance and the rule of law, at national, regional and international levels. ICTs can be used to promote economic growth and enterprise development. Infrastructure development, human capacity building, information security and network security are critical to achieve these goals. We further recognize the need to effectively confront challenges and threats resulting from use of ICTs for purposes that are inconsistent with objectives of maintaining international stability and security and may adversely affect the integrity of the infrastructure within States, to the detriment of their security. It is necessary to prevent the abuse of information resources and technologies for criminal and terrorist purposes, while respecting human rights”,

aware

a) that ITU and other international organizations, through a variety of activities, are examining issues related to building confidence and security in the use of ICTs including stability and measures to combat spam, malware, transmission of unsolicited content etc., and to protect personal data and privacy;

b) that Study Group 17 of the Telecommunication Standardization Sector (ITU-T) and other relevant ITU study groups continue to work on technical means for the security of information and communication networks, in accordance with Resolutions 50, 51, 52 (Florianópolis, 2004) of the World Telecommunication Standardization Assembly;

noting

a) that, as an intergovernmental organization with private sector participation, ITU is well positioned to play an important role, together with other international bodies and organizations, in addressing threats and vulnerabilities, which affect efforts to build confidence and security in the use of ICTs;

b) § 35 and § 36 of the Geneva Declaration of Principles and paragraph § 39 of the Tunis Agenda, on building confidence and security in the use of ICTs;

c) that, although there are no universally agreed upon definitions of spam and other terms in this sphere, spam was characterised by ITU-T Study Group 2 at its June 2006 session, as a term commonly used to describe unsolicited electronic bulk communications over e-mail or mobile messaging (SMS, MMS), usually with the objective of marketing commercial products or services, *resolves*

to give this work a high priority within ITU, in accordance with its competences and expertise,

instructs the Secretary-General and the Directors of the Bureaux

1 to review:

i) the work done so far by ITU and other relevant organizations, and initiatives to address existing and future threats in order to build confidence and security in the use of ICTs, such as the issue of countering spam;

ii) the progress achieved in the implementation of this resolution and in the role of ITU as moderator/facilitator for WSIS action line C5 with the help of the advisory groups, consistent with the ITU Constitution and Convention;

2 to facilitate access to tools required for enhancing confidence and security in the use of ICTs for all Member States, consistent with WSIS provisions on universal and non-discriminatory access to ICTs for all nations;

3 to continue the Cybersecurity Gateway as a way to share information on national, regional and international cybersecurity-related initiatives worldwide;

4 to report annually to the Council on these activities and to make proposals as appropriate,

instructs the Director of the Telecommunication Standardization Bureau

1 to intensify work within existing ITU-T study groups in order to:

i) address existing and future threats and vulnerabilities affecting efforts to build confidence and security in the use of ICTs by developing recommendations, as appropriate;

ii) seek ways to enhance the exchange of technical information in these fields, promote implementation of emerging protocols and standards that further enhance security, and promote international cooperation among appropriate entities;

2 to continue collaboration with relevant organizations with a view to exchanging best practices and disseminating information through, for example, joint workshops and training sessions;

instructs the Director of the Telecommunication Development Bureau

1 to develop, consistent with the results of WTDC-06 and the subsequent meeting pursuant to Resolution 45 (Doha, 2006) of that conference, the projects for enhancing cooperation on cybersecurity and combating spam responding to the needs of developing countries, in close collaboration with the relevant partners;

2 to provide the necessary financial and administrative support for these projects within existing resources, and to seek additional resources (in cash and in kind) for the implementation of these projects through partnership agreements;

3 to ensure coordination of these projects within the context of ITU's overall activities in its role as moderator/facilitator for WSIS action line C5;

4 to coordinate these projects with the activities and programmes of ITU-D study groups on this topic;

5 to continue collaboration with relevant organizations with a view to exchanging best practices and disseminating information through, for example, joint workshops and training sessions;

6 to report annually to the Council on these activities and make proposals as appropriate,

requests the Council

to include the report of the Secretary General in the documents sent to Member States in accordance with No. 81 of the Convention;

invites ITU Member States, Sector Members and Associates

1 to participate actively in the ongoing work of the relevant ITU study groups;

2 to develop, as appropriate, the necessary relevant legislation, noting in particular regional initiatives including, but not limited to, the Council of Europe's Convention on Cybercrime;

3 to make contributions on this subject in ITU-D Study Group 1 and participate in the ongoing activities of the BDT projects;

4 to contribute to building confidence and security in the use of ICTs at the national, regional and international levels, by undertaking activities as outlined in § 12 of the Geneva Plan of Action.

World Telecommunication Development Conference Resolution 45 (Doha, 2006): Mechanisms for enhancing cooperation on cybersecurity, including combating spam

The World Telecommunication Development Conference (Doha, 2006),

recalling

a) the noble principles, aims and objectives embodied in the United Nations Charter and the Universal Declaration of Human Rights;

b) its fundamental support for Programme 3 (e-strategies and ICT-applications), confirming that the latter shall have primary responsibility for Action Line C5 in the Tunis Agenda (Building confidence and security in the use of ICTs);

c) the provisions of §§ 35, 36 and 37 of the Geneva Declaration of Principles;

d) the provisions of § 15 of the Tunis Commitment,

considering

a) the role of ICTs as effective tools to promote peace, security and stability and to enhance democracy, social cohesion, good governance and the rule of law, and the need to confront challenges and threats resulting from the abuse of this technology, including for criminal and terrorist purposes, while respecting human rights (§ 15 of the Tunis Commitment);

b) the need to build confidence and security in the use of ICTs (§ 39 of the Tunis Agenda) and to prosecute cybercrime, at national and regional levels, noting existing frameworks, for example, Resolutions 55/63 and 56/121 of the General Assembly of the United Nations on "Combatting the criminal misuse of information technologies" and regional initiatives including, but not limited to, the Council of Europe's

Convention on Cybercrime;

c) that the considerable losses which ICT systems have incurred from the growing problem of cybercrime worldwide should alarm the entire international community, and ITU in particular;

d) the need, through a multi-pronged approach, including international cooperation, to counter the problem associated with cybersecurity, including spam, which has not been given the necessary priority as called for in the Tunis Agenda (§ 41);

e) the reasons behind the adoption of Resolution 37 (Istanbul, 2002) on bridging the digital divide, having regard to the action lines referenced in § 108 of the Tunis Agenda, including "Building confidence and security in the use of ICTs",

recalling

a) desire and commitment of all concerned to build a people-centred, inclusive and development oriented information society, premised on the purposes and principles of the Charter of the United Nations, international law and multilateralism, and respecting fully and upholding the Universal Declaration of Human Rights, so that people everywhere can create, access, utilize and share information and knowledge, to achieve their full potential and to attain the internationally agreed development goals and objectives, including the Millennium Development Goals;

b) the provisions of §§ 4, 5 and 55 of the Geneva Declaration of Principles, and that freedom of expression and the free flow of information, ideas and knowledge are beneficial to development;

c) that the Tunis Summit represented a unique opportunity to raise awareness of the benefits that ICTs can bring to humanity and the manner in which they can transform people's activities, interaction and lives, and thus increase confidence in the future,

recognizing

a) the provisions for privacy and freedom of expression as contained in the relevant parts of the Universal Declaration of Human Rights (§ 42 of the Tunis Agenda);

b) the need to safeguard the ethical dimensions of the information society in accordance with the Geneva Declaration of Principles and Action Plan (§ 43 of the Tunis Agenda), the need to counter terrorism (§ 44 of the Tunis Agenda) and the importance of continuity and stability of the internet (§ 45 of the Tunis Agenda), while ensuring respect for privacy and the protection of personal information and data (§ 46 of the Tunis Agenda);

c) the need to effectively confront challenges and threats resulting from use of ICTs for purposes that are inconsistent with objectives of maintaining international stability and security and may adversely affect the integrity of the infrastructure within States to the detriment of their security, and that it is necessary to work to prevent the abuse of information resources and technologies for criminal and terrorist purposes, while respecting human rights;

d) the role of ICTs in the protection of children and in enhancing their development and that action to protect children from abuse and defend their rights in the context of ICTs should be strengthened, emphasizing that the best interests of the child are a key consideration,

noting

a) that Resolution 50 (Florianópolis, 2004) of the World Telecommunication Standardization Assembly on cybersecurity is confined solely to the study of technical aspects for reducing the impact of this phenomenon;

b) that spam is a significant and growing problem for users, networks and the internet as a whole, and spam and cybersecurity should be dealt with at appropriate national and international levels,

urges Member States

to provide the support necessary for implementation of this resolution, *resolves to instruct the Director of the Telecommunication Development Bureau*

1 to organize, in conjunction with Programme 3 and based on member contributions, meetings of Member States and Sector Members to discuss ways to enhance cybersecurity including, *inter alia*, a memorandum of understanding to enhance cybersecurity and combat spam amongst interested Member States;

2 to report the results of these meetings to the 2006 plenipotentiary conference.

Resolution 45 (WTDC-06) Follow-Up: Report of the Meeting on Mechanisms for Cooperation on Cybersecurity and Combating Spam, Geneva, 31 August – 1 September 2006

1. Introduction

WTDC2006 adopted Resolution 45 which called for the Director of the BDT to organize a meeting in conjunction with Doha Action Plan Programme 3 on mechanisms for cooperation on Cybersecurity and combating spam and to report to the 2006 ITU Plenipotentiary Conference the results of this meeting.

The meeting was opened by the Director of the BDT Mr. Hamadoun TOURÉ who in his opening remarks stressed the importance of Cybersecurity, its broad scope and the importance for the meeting to arrive at concrete solutions that will address the needs of all membership taking into account specific challenges faced by developing countries and existing solutions.

Mr. Makhtar FALL of Senegal chaired the meeting assisted by Mr. Alexander NTOKO of BDT. The Chair presented the agenda which was adopted. In his opening remarks, the Chairman highlighted the challenges faced by developing countries in this domain and called for a spirit of collaboration and consensus to arrive at concrete results.

Some 50 participants including delegates from 24 Member States, Sector members, UN Office on Drugs and Crime, Council of Europe, European Commission, World Bank and ITU staff (BDT, TSB and General Secretariat) attended the two-day event. The meeting was organized in all six (6) ITU languages. For further information and background documents, please see http://www.itu.int/ITU-D/cybersecurity.

2. Presentation of input documents

The adoption of the agenda and opening remarks from the Chair were followed by a presentation by BDT on the mandate of the Development Sector in the domain of Cybersecurity and combating Spam. Other background and reference documents were used as sources for discussions and inspiration. Presentations on national, regional and multi-lateral and international initiatives on Cybersecurity and combating spam were made by Australia, Cisco Systems, Council of Europe, European Commission, Lithuania, Niger, Russian Federation, Sudan, Syrian Arab Republic on behalf of the Arab States, United Kingdom, United States of America, Uzbekistan and World Bank.

The presentations highlighted initiatives in capacity building, legislation, technologies, incident response, policies and strategies, partnerships, and enforcement. In addition to existing initiatives, new ones including proposals for the establishment of a Memorandum of Understanding were presented by delegates from developing countries. The contributions confirmed the existence of several initiatives most of them undertaken by developed countries with limited participation of developing countries.

3. Discussions and Analysis

Delegates commented on the presentations and made a several proposals on possible ways forward. The need for cooperation and collaboration was highlighted in most presentations and discussions. Delegates agreed on the necessity to leverage existing sources of expertise to meet the needs of developing countries. Most of the presentations and discussions identified areas where it was considered necessary for actions to be undertaken at the national, regional and international levels.

Activities in capacity building, national legislation, national policies and strategies, public/private partnerships, enforcement mechanisms, information exchange, establishment of national focal points, incident response and technological solutions were identified as important for cooperation amongst Member States in cybersecurity and combating spam. There was a general agreement that it was necessary for some mechanisms to be put in place to provide assistance to countries that requested it. During the discussions and analysis of the challenges1 and existing initiatives, it was apparent that even though cyber threats and spam need to be addressed at a global level, the specific requirements especially those of developing countries have to be addressed. Participation of all interested countries (developing and developed) in a global and multi-lateral initiative would require all countries to meet some minimum national requirements in areas such as legislation, human and institutional capacity and appropriate national policies and strategies.

The presentations and discussions resulted in the identification of a number of areas where future activities should be undertaken by ITU-D to meet challenges faced by developing and least developed countries.

While many of the activities were to be undertaken at the national level, it was agreed that there was need for cooperation and coordination amongst the various stakeholders and initiatives and that ITU-D should play a role to facilitate the implementation of the actions that are part of its mandate and requested by Member States. It was suggested that certain practical tasks could be identified in this context and that ITU experience and expertise be utilized in undertaking them.

In line with the spirit and objective of Resolution 45, and considering the general agreement that some areas of activity needed coordination beyond existing frameworks, the main focus was now to agree on the type of mechanism to be put in place for ITU-D to provide the required assistance to developing countries. Three options were tabled for discussion.

a) A memorandum of understanding amongst interested Member States with ITU Secretary-General as the depository.

b) Technical cooperation framework(s) between ITU and interested Member States and partners.

c) A project on the implementation of Resolution 45 for interested countries and with the participation of recognized sources of expertise.

All three options are aimed at putting in place mechanisms to enhance cooperation amongst interested stakeholders using expertise and experiences of existing entities and initiatives. All three options would be non-binding to Member States, open to interested countries and focused on addressing the needs of countries that are not part of existing frameworks.

One of the important considerations taken into account was the fact that ITU-D mandate in Cybersecurity and combating spam has in particular three main components – Doha Action Plan Programme 3, ITU-D Study Group 1 Question 22 and WTDC2006 Resolution 45. The output and recommendations made by this meeting were therefore aimed at proposals that were not already part of decisions agreed to by Membership at the WTDC2006 but to work towards mechanisms that were not part of existing decisions but necessary and requested by developing countries.

4. Recommendations for future actions

As a result of WSIS Thematic meeting on countering Spam, the following areas were considered important for the work in the domain of cybersecurity and combating spam.

Strong legislation

Development of technical measures

The establishment of industry partnerships, especially with Internet Service Providers, mobile carriers and direct marketing associations

The education of consumers and industry players about anti-spam measures and Internet security practices

International cooperation at the level of governments, industry, consumer, business and anti-spam groups, to allow a global and coordinated approach to the problem.

In addition to the list above, during discussions and presentations the areas below were identified not in any order of priority as also important for cooperation and assistance to Member States, in which the ITU-D may be involved with entities with recognized expertise in the domain of Cybersecurity and combating spam:

a. Building basic awareness

b. Appropriate national legislation

c. Human and institutional capacity building

d. Enforcement (capacity building domain)

e. National policies and strategies on cybersecurity

f. Exchange of information between countries and relevant stakeholders

g. Establishment of national focal points

h. Monitoring and evaluation of progress on existing initiatives

i. Incident response, watch and warning.

j. Assessment of cybersecurity vulnerabilities and threats.

k. Effective tools and applications for network and cybersecurity

l. Partnerships

m. International cooperation

The meeting arrived at a consensus that ITU-D should play a key role in linking existing initiatives and provide a unifying framework bringing together these initiatives with the objective of addressing the needs of developing countries.

The meeting invited ITU-D to take account as appropriate of the relevant work of other stakeholders with recognized areas of expertise, such as ITU-T, London Action Plan, World Bank, Seoul-Melbourne Memorandum of Understanding (MoU), United Nations Office on Drugs and Crime, Council of Europe Convention on Cybercrime, Asia-Pacific Economic Cooperation Telecommunications and Information Working Group (APEC TEL), Organisation for Economic Co-operation and Development (OECD) anti-spam efforts and other relevant partners.

For the above-listed areas, the meeting recommended that the BDT under the coordination of Programme 3 should develop a project as the mechanism for the implementation of WTDC06 Resolution 45. Based on the needs and priorities of developing countries that request ITU assistance in this domain, the project should take account as appropriate, of recognised sources expertise and exiting initiatives including but not limited to: ITU-T, London Action Plan, World Bank, Seoul-Melbourne Memorandum of Understanding (MoU), United Nations Office on Drugs and Crime, Council of Europe Convention on Cybercrime, Asia-Pacific Economic Cooperation Telecommunications and Information Working Group (APEC TEL), Organisation for Economic Co-operation and Development (OECD) anti-spam efforts and other relevant partners.

Regarding the Project:

- Titled “Project for enhancing cooperation on Cybersecurity and combating spam”, the project will have the duration of 4 years beginning from 2007 and be part of BDT Operational Plan for 2007.
- Annual reports will be made to ITU Council sessions on progress achieved in its implementation.
- The project in its implementation should take into account decisions of the WTDC06 on the mandate of the Development Sector in Cybersecurity and combating spam.

- The project should aim primarily at providing assistance to developing countries in the areas identified above by the meeting as vital for cooperation in the domain of Cybersecurity and combating spam.
- With regards to relevant legislation, take into account as appropriate, the relevant work of the Council of Europe when assisting countries in the development of national legislation in line with the Convention on Cybercrime
- Implementation of activities under the framework of this project should be based on expressed requests of countries with emphasis on developing countries.
- After the development of the project, it should be presented to potential funding entities including Member States, private sector and international organizations such as the World Bank and the European Commission.

Resolution 123 (Rev. Antalya, 2006): Bridging the standardization gap between developing and developed countries

The Plenipotentiary Conference of the International Telecommunication Union (Antalya, 2006),

considering

a) that "the Union shall in particular facilitate the worldwide standardization of telecommunications, with a satisfactory quality of service" (Article 1 of the ITU Constitution);

b) that, in connection with the functions and structure of the Telecommunication Standardization Sector (ITU-T), in Article 17, the Constitution indicates that those functions shall be "..., bearing in mind the particular concerns of the developing countries, to fulfill the purposes of the Union...";

c) that, under the Strategic Plan for the Union 2008-2011, ITU-T is to work to provide support and assistance to the membership, mainly to developing countries, in relation to standardization matters, information and communication network infrastructure and applications, and in particular with respect to (a) bridging the digital divide; and (b) providing training and producing relevant training materials for capacity building,

considering further

a) that the World Telecommunication Standardization Assembly adopted Resolutions 44 (Florianópolis, 2004), 53 (Florianópolis, 2004) and 54 (Florianópolis, 2004) as well as Resolution 17 (Rev. Florianópolis, 2004) to assist in bridging the standardization gap between developing and developed countries;

b) that the World Telecommunication Development Conference adopted Resolution 47 (Doha, 2006), which calls for activities to enhance knowledge and effective application of Recommendations of ITU-T and of the ITU Radiocommunication Sector (ITU-R) in developing countries, and Resolution 37 (Rev. Doha, 2006) which recognizes the need to create digital opportunities in developing countries,

recalling

that the Geneva Plan of Action and Tunis Agenda for the Information Society of the World Summit on Information Society (WSIS) emphasize efforts to overcome the digital divide and development divides,

noting

the following goals in the Strategic Plan for the Union for 2008-2011, adopted in Resolution 71 (Rev. Antalya, 2006) of this conference:

- Goal 1: Maintaining and extending international cooperation among all Member States and with relevant regional organizations for the improvement and rational use of information and communication infrastructure of all kinds, taking the appropriate leading role in United Nations system initiatives on ICTs, as called for by the relevant WSIS outcomes;

- Goal 2: Assisting in bridging the national and international digital divides in ICTs, by facilitating interoperability, interconnection and global connectivity of networks and services, and by playing a leading role, within its mandate, in the multistakeholder process for the follow-up and implementation of the relevant WSIS goals and objectives.;

- Goal 6: Disseminating information and know-how to provide the membership and the wider community, particularly developing countries, with capabilities to leverage the benefits of, *inter alia*, private-sector participation, competition, globalization, network security and efficiency and technological change in their ICT sector, and enhancing the capacity of ITU Member States, in particular developing countries, for innovation in ICTs,

recognizing

a) the continued shortage of human resources in the standardization field in developing countries, resulting in a low level of developing-country participation in meetings of ITU-T and of ITU-R and, consequently, in the standards-making process, leading to difficulties when interpreting ITU-T and ITU-R Recommendations;

b) ongoing challenges relating to capacity building, in particular for developing countries, in the light of rapid technological innovation and increased convergence,

taking into account

a) that developing countries could benefit from improved capability in the application and development of standards;

b) that ITU-T and ITU-R activities and the telecommunication/ICT market could also benefit from better involvement of developing countries in standard-making and standards application;

c) that initiatives to assist in bridging the standardization gap are intrinsic to, and are a high priority task of, the Union,

resolves to instruct the Secretary-General and the Directors of the three Bureaux

1 to work closely with each other on the follow-up and implementation of this resolution, as well as the operative paragraphs of Resolutions 44 (Florianópolis, 2004), 54 (Florianópolis, 2004) and 17 (Rev. Florianópolis, 2004) and Resolution 47 (Doha, 2006) that assist in bridging the standardization gap between developing and developed countries;

2 to maintain, to the extent practicable, a close coordination mechanism among the three Sectors at the regional level through ITU regional offices;

3 to further collaborate with the relevant regional organizations and support their work in this area,

invites Member States and Sector Members

to make voluntary contributions to the fund for bridging the standardization gap, as well as to undertake concrete actions to support the actions and initiatives of ITU in this matter.

World Telecommunication Standardization Assembly (WTSA) Resolution 50 (Florianopolis, 2004): Cybersecurity

The World Telecommunication Standardization Assembly (Florianópolis, 2004),

considering

a) the crucial importance of the information and communication infrastructure to practically all forms of social and economic activity;

b) that the legacy public switched telephone network (PSTN) has a level of inherent security properties because of its hierarchical structure and built-in management systems;

c) that IP networks provide reduced separation between user components and network components if adequate care is not taken in the security design and management;

d) that the converged legacy networks and IP networks are therefore potentially more vulnerable to intrusion if adequate care is not taken in the security design and management;

e) that the type and number of cyberincidents, including attacks from worms, viruses, malicious intrusions and thrill-seeker intrusions are on the increase,

recognizing

the resolves of Resolution 130 (Marrakesh, 2002) of the Plenipotentiary Conference to strengthen the role of ITU in information and communication network security, and the instruction to intensify work within ITU study groups,

recognizing further

the emphasis of this assembly to focus the network security work of the ITU Telecommunication Standardization Sector (ITU-T),

noting

the vigorous activity and interest in the development of security standards and Recommendations in ITU-T Study Group 17 and in other standardization bodies, including the Global Standards Collaboration group,

resolves

1 that ITU-T evaluate existing and evolving new Recommendations, and especially signalling and communications protocol Recommendations, with respect to their robustness of design and potential for exploitation by malicious parties to interfere destructively with their deployment in the global information and communication infrastructure;

2 that ITU-T continue to raise awareness, within its area of operation and influence, of the need to defend information and communication systems against the threat of cyberattack, and continue to promote cooperation among appropriate entities in order to enhance exchange of technical information in the field of information and communication network security,

further resolves

to forward to the Telecommunication Standardization Advisory Group (TSAG) the report of the Cybersecurity Symposium held on 4 October 2004 in Florianópolis, for its consideration and follow-up as appropriate,

instructs the Director of the Telecommunication Standardization Bureau

to develop, in consultation with the chairman of TSAG and the appropriate study group chairmen, a plan to undertake the abovementioned evaluation of relevant Recommendations at the earliest possible time considering resources available and other priorities, and to provide updates of the progress regularly to TSAG,

further instructs the Director of the Telecommunication Standardization Bureau

1 to include in the annual report to the Council specified in Resolution 130 (Marrakesh, 2002) of the Plenipotentiary Conference the progress in the evaluations under resolves above;

2 to continue to take appropriate action to publicize the need to defend information and communication networks against the threat of cyberattack, and to cooperate with other relevant entities in these efforts;

3 to liaise with other bodies active in this field, such as the International Organization for Standardization (ISO) and the Internet Engineering Task Force (IETF),

invites Member States, Sector Members and Associates, as appropriate,

to participate actively in the implementation of this resolution and the associated actions.

World Telecommunication Standardization Assembly (WTSA) Resolution 51 (Florianopolis, 2004): Countering spam

The World Telecommunication Standardization Assembly (Florianópolis, 2004),

recognizing

that the “Declaration of Principles” of the World Summit on the Information Society (WSIS) states that:

37. Spam is a significant and growing problem for users, networks and the Internet as a whole. Spam and cybersecurity should be dealt with at appropriate national and international levels,

recognizing further

that the WSIS "Plan of Action" states that:

12. Confidence and security are among the main pillars of the information society.

d) Take appropriate action on spam at national and international levels,

considering

a) relevant provisions of the basic instruments of ITU;

b) that agreed measures to combat spam fall within Goal 4 of the strategic plan for the Union for 2004-2007 (Part I, clause 3) set out in Resolution 71 (Rev. Marrakesh, 2002) of the Plenipotentiary Conference;

c) Resolution 52 on countering spam by technical means;

d) the report of the chairman of the ITU WSIS thematic meeting on countering spam, which advocated a comprehensive approach to combating spam, namely:

i) strong legislation,

ii) the development of technical measures,

iii) the establishment of industry partnerships,

iv) education, and

v) international cooperation,

instructs the Director of the Telecommunication Standardization Bureau, in cooperation with the Directors of the other Bureaux and the Secretary-General

to prepare urgently a report to the Council on relevant ITU and other international initiatives for countering spam, and to propose possible follow-up actions for consideration by the Council,

invites Member States and Sector Members

to contribute to this work,

further invites Member States

to take appropriate steps within their national legal frameworks to ensure that appropriate and effective measures are taken to combat spam.

World Telecommunication Standardization Assembly (WTSA) Resolution 52 (Florianopolis, 2004): Countering spam by technical means

The World Telecommunication Standardization Assembly (Florianópolis, 2004),

considering

a) that spam has become a widespread problem causing loss of revenue to Internet service providers, telecommunication operators, mobile telecommunication operators and business users, as well as other problems to users in general;

b) the report of the chairman of the ITU World Summit on the Information Society thematic meeting on countering spam, which advocated a comprehensive approach to combating spam, namely:

i) strong legislation,

ii) the development of technical measures,

iii) the establishment of industry partnerships,

iv) education, and

v) international cooperation;

c) that technical measures to counter spam represent one of those approaches mentioned in b) above;

d) that many countries, in particular countries with economies in transition, developing countries, and especially least developed countries, need help when it comes to countering spam;

e) that spamming is at times used for criminal, fraudulent or deceptive activities;

f) the availability of relevant ITU-T Recommendations, which could provide guidance for future development in this area, particularly with regard to lessons learned,

recognizing

a) relevant provisions of the basic instruments of ITU;

b) that spam creates telecommunication network security problems, including by being a vehicle for spreading viruses, worms, etc.;

c) that spam is a global problem that requires international cooperation in order to find solutions;

d) that addressing the issue of spam is a matter of urgency,

instructs the relevant study groups

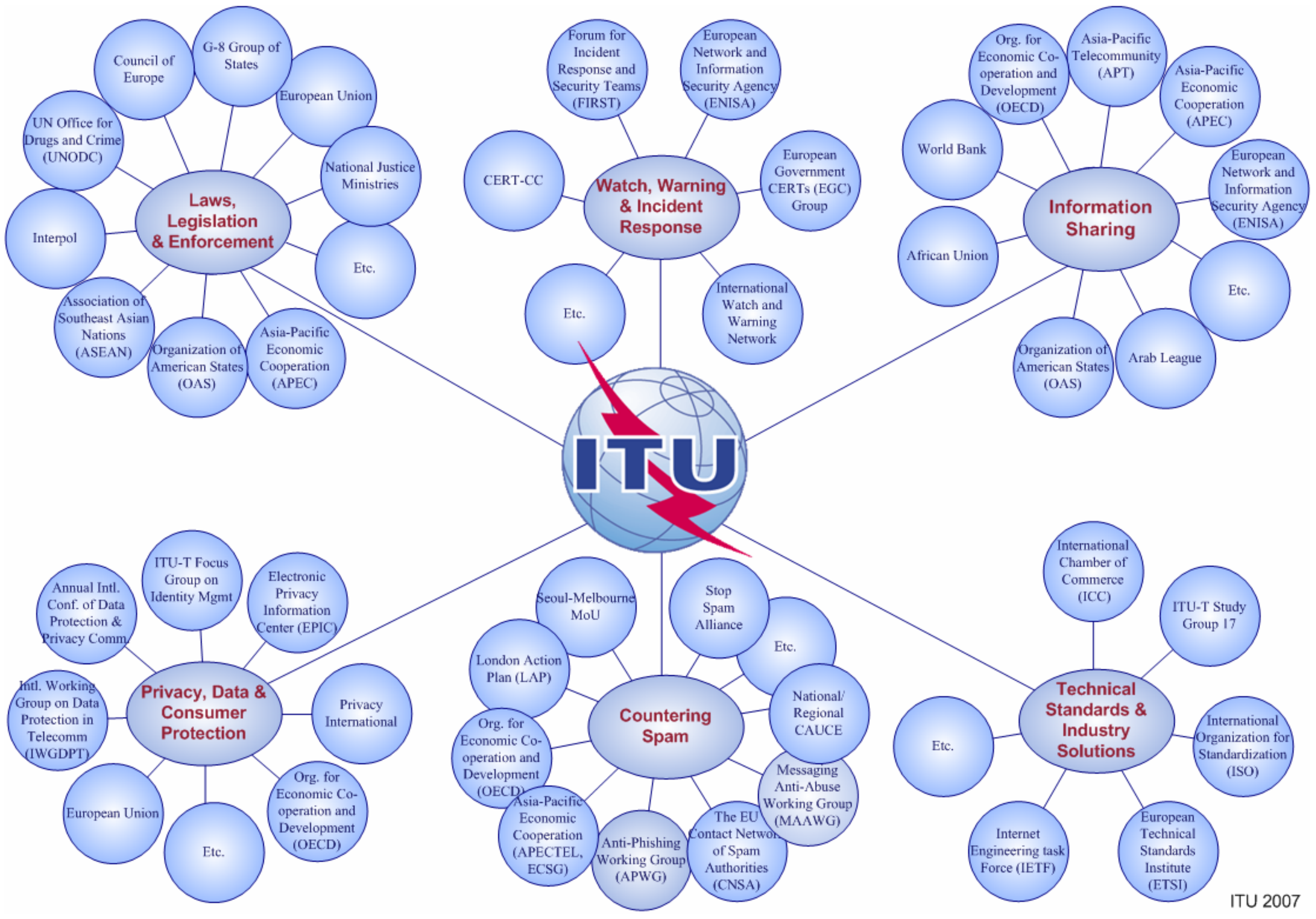
in cooperation with the Internet Engineering Task Force (IETF) and other relevant groups, to develop, as a matter of urgency, technical Recommendations, including required definitions, on countering spam, as appropriate, and to report regularly to the Telecommunication Standardization Advisory Group on their progress,

instructs the Director of the Telecommunication Standardization Bureau

to provide all necessary assistance with a view to expediting such efforts, and to report on this to the Council.

Annex C: Organisations Involved in Cybersecurity Initiatives

Organizations Involved in Cybersecurity Initiatives


ITU
Laws, Legislation & Enforcement
Council of Europe
G-8 Group of States
European Union
UN Office for Drugs and Crime (UNODC)
National Justice Ministries
Interpol
Etc.
Association of Southeast Asian Nations (ASEAN)
Organization of American States (OAS)
Asia-Pacific Economic Cooperation (APEC)
Watch, Warning & Incident Response
Forum for Incident Response and Security Teams (FIRST)
European Network and Information Security Agency (ENISA)
CERT-CC
European Government CERTs (EGC) Group
Etc.
International Watch and Warning Network
Information Sharing
Org. for Economic Co-operation and Development (OECD)
Asia-Pacific Telecommunity (APT)
Asia-Pacific Economic Cooperation (APEC)
World Bank
European Network and Information Security Agency (ENISA)
African Union
Etc.
Organization of American States (OAS)
Arab League
Privacy, Data & Consumer Protection
Annual Intl. Conf. of Data Protection & Privacy Comm.
ITU-T Focus Group on Identity Mgmt
Electronic Privacy Information Center (EPIC)
Intl. Working Group on Data Protection in Telecomm (IWGDPT)
Privacy International
European Union
Etc.
Org. for Economic Co-operation and Development (OECD)
Countering Spam
Seoul-Melbourne MoU
Stop Spam Alliance
Etc.
London Action Plan (LAP)
National/ Regional CAUCE
Org. for Economic Co-operation and Development (OECD)
Messaging Anti-Abuse Working Group (MAAWG)
Asia-Pacific Economic Cooperation (APECTEL, ECSG)
Anti-Phishing Working Group (APWG)
The EU Contact Network of Spam Authorities (CNSA)
Technical Standards & Industry Solutions
International Chamber of Commerce (ICC)
ITU-T Study Group 17
Etc.
International Organization for Standardization (ISO)
Internet Engineering task Force (IETF)
European Technical Standards Institute (ETSI)
ITU 2007