ITU-T Network Security Initiatives

Michael Harrop

The Cottingham Group

SG17 Rapporteur, Communications Security Project

ITU-T

Overview of Presentation

- Show the context of ITU-T security standards activities
- Highlight some of key areas of security work in ITU-T and SG17 in particular
- Give a quick overview of some related activities
- Report in a little more detail on some of the results being achieved

Context of ITU-T security standards work

Issues and Challenges

- Constant evolution of the nature of cyberthreats
- Vulnerabilities in software and hardware applications and services
- Low entry barriers for cyber-criminals
- Increasing sophistication of cybercrime
- Loopholes in current legal frameworks
- Absence of appropriate organizational structures
- Inadequate cooperation among various stakeholders
- Global problem which cannot be solved by any single entity (country or organization) –

ITU-T is working with many international partners to address these issues

High Level Security Drivers

- ITU Plenipotentiary Conference (PP-02) & (PP-06)
  - Intensify efforts on security
- World Telecommunications Standardization Assembly (WTSA-04)
  - Security robustness of protocols
  - Combating/Countering spam
- World Summit on the Information Society (WSIS-05)
  - Cyber security

ITU-T Security Work

- Most (but not all) ITU-T security work is done in SG17
- SG17 is the Lead Study Group on security
- Other SGs address the security aspects of their own work

ITU-T Study Group 17

Security, Languages and Telecommunication Software

- Q.4/17, Communications Systems Security Project
- Q.5/17, Security Architecture and Framework
- Q.6/17, Cyber Security
- Q.7/17, Security Management
- Q.8/17, Telebiometrics
- Q.9/17, Secure Communication Services
- Q.17/17, Countering Spam by Technical Means
- Q.2/17, Directory Services, Directory Systems and Public-key/Attribute Certificates

Working Party 2/17 Work Areas

Telecom Systems

Q.8/17

Telebiometrics
* Multimodal model framework
* System mechanism
* Protection procedure

Q.7/17

Security Management
* ISMS-T
* Incident management
* Risk assessment methodology

Q.5/17

Security Architecture and Framework
* Architecture,
* Model,
* Concepts,
* Frameworks

Secure Communication Services
* Secure mobile communications
* Home network security
* Web services security

Q.9/17

Cyber Security
* Vulnerability information sharing…
* Incident handling operations
* Identity management

Q.6/17

Countering spam by technical means
* Technical anti-spam measures

Q.17/17

Q.4/17

Communications System Security Project *Vision, Project, Roadmap, …

Overview of current security Questions and Recommendations under development

Q4/17: Communications Systems Security Project

- Overall Security Coordination and Vision
- Outreach and promotional activities
  - ICT Security Standards Roadmap
  - Security Compendium
  - ITU-T Security manual
  - Survey of needs of Developing Countries
- Focus Group on Security Baseline For Network Operators (Completed)

Q5/17: Security Architecture and Framework

- To investigate new security requirements and solutions and how security architectures and frameworks can be developed to achieve cost-effective comprehensive security solutions that can be applied to various types of networks, services and applications in a multi-vendor environment

- Also responsible for maintenance and enhancements of X.800 series Recommendations

Examples of Q5/17 Recommendations

- X.805, *Security Architecture for Systems Providing End-to-end Communications* Approved in 2003
- ISO/IEC Standard 18028-2, *Network security architecture*
  - Published in 2006
- X.1031, *Security architecture aspects of end users and networks in telecommunications*
- X.1035, *Password-authenticated key exchange (PAK) protocol*
  - Approved in 2006
- Supplement to X.800-X.849, *Guidelines for implementing system and network security*

Q6/17: Cyber Security

- Definition of Cybersecurity
- Security of Telecommunications Network Infrastructure
- Security Knowledge and Awareness of Telecom Personnel and Users
- Security Requirements for Design of New Communications Protocol and Systems
- Communications relating to Cybersecurity
- Security Processes – Life-cycle Processes relating to Incident and Vulnerability
- Security of Identity in Telecommunication Network
- Legal/Policy Considerations
- IP traceback technologies
- Authentication Assurance

Q.6/17 Completed Recommendations

No.	Title
X.1205	Overview of Cybersecurity
X.1206	A vendor-neutral framework for automatic checking of the presence of vulnerabilities information update
X.1207	Guidelines for Internet Service Providers and End-users for Addressing the Risk of Spyware and Deceptive Software
X.1250*	Requirements for global identity management trust and interoperability
X.1303	Common Alerting Protocol (CAP 1.1)

* Currently in the approval process

ITU-T

Q7/17: Security Management

- The scope of this question is to provide GUIDELINES and BASELINES for Information Security Management to be appropriately applied for telecommunications organizations.

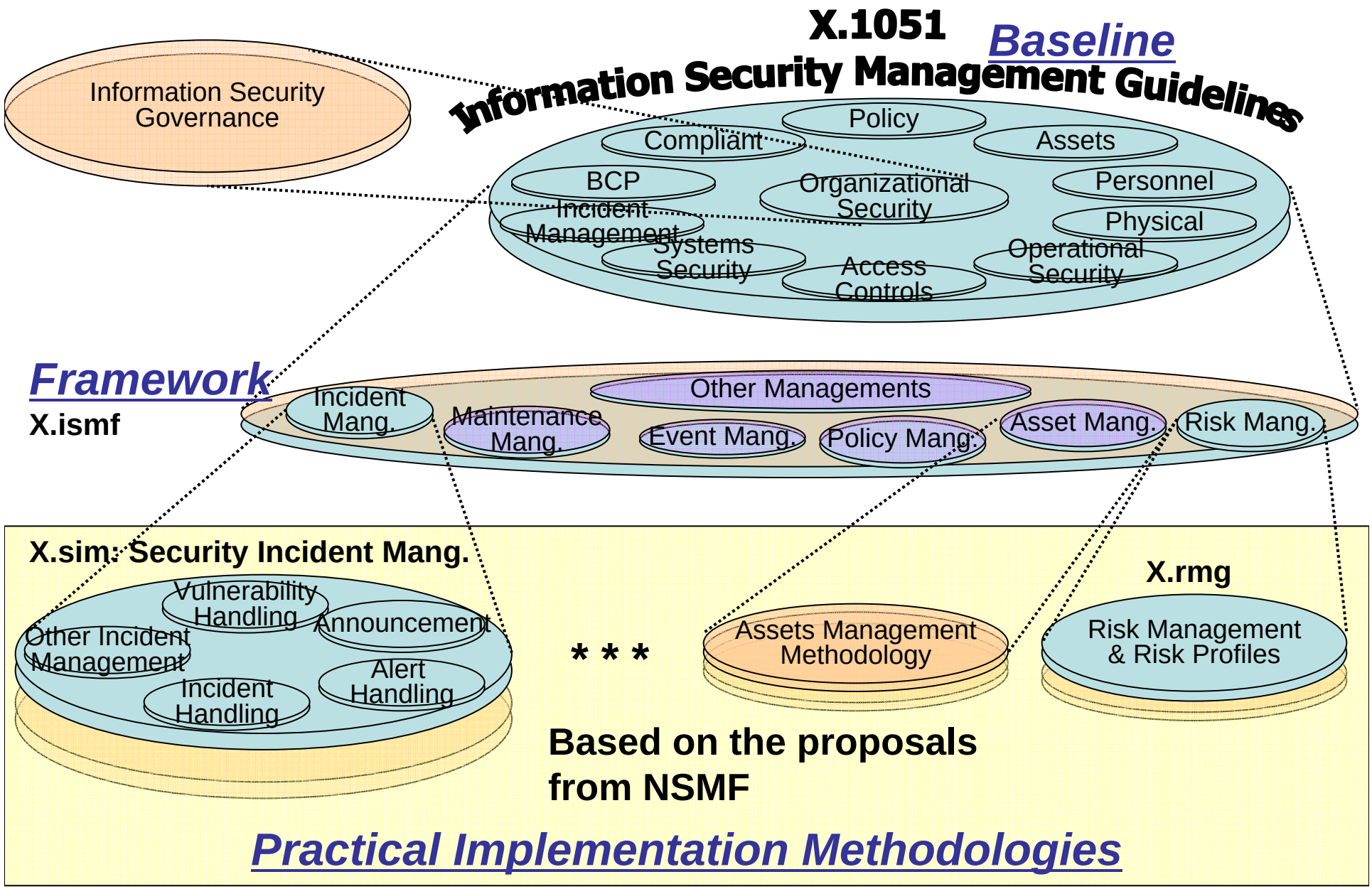
- Includes:
  - information security management guidelines (baseline)
  - information incident management guidelines
  - risk management and risk profiles guidelines
  - assets management guidelines
  - policy management guidelines
  - information security governance

Q.7/17 Highlights

Recommendations

No.	Title
X.1051	Information security management guideline for telecommunications organizations based on ISO/IEC 27002
X.rmg*	Risk management and risk profile guide
X.sim*	Security incident management guidelines for telecommunications
X.ismf*	Information Security Management Framework for Telecommunications

* Currently under development


X.1051
Baseline
Information Security Management Guidelines
Information Security Governance
Policy
Compliant
Assets
BCP
Organizational Security
Personnel
Incident Management
Physical
Systems Security
Operational Security
Access Controls
Framework
X.ismf
Other Managements
Incident Mang.
Maintenance Mang.
Event Mang.
Policy Mang.
Asset Mang.
Risk Mang.
X.sim: Security Incident Mang.
Vulnerability Handling
Announcement
Other Incident Management
Alert Handling
Incident Handling
* * *
Assets Management Methodology
X.rmg
Risk Management & Risk Profiles
Based on the proposals from NSMF
Practical Implementation Methodologies

ITU-T

Q8/17: Telebiometrics

- Focuses on how identification and authentication of users be improved by the use of safe and secure telebiometric methods and how issues of biometric authentication technologies for telecommunications can be identified.
- Builds on existing work relating to personal identification and authentication using telebiometrics
- It is being undertaken in close cooperation with related standards work being undertaken in other SDOs.

Q8/17 Approved Recommendations

No.	Title
X.1082	Telebiometrics related to human physiology
X.1083	BioAPI Interworking Protocol
X.1084	Telebiometrics system mechanism – Part 1: General biometric authentication protocol and system model profiles on telecommunication systems
X.1088	Telebiometrics digital key – A framework for biometric digital key generation and protection
X.1089	Telebiometrics authentication infrastructure

Q9/17: Secure Communication Services

- Develop a set of standards for secure application services, including:
  - Mobile security
  - Home network security
  - Web Services security
  - Secure application services
  - NID/USN security Under study
  - Multicast security Under study
  - IPTV security Under study

Q9/17 Approved Recommendations

Mobile Security

- X.1121, Framework of security technologies for mobile end-to-end data communications Approved 2004
- X.1122, Guideline for implementing secure mobile systems based on PKI Approved 2004
- X.1123, General security value added service (policy) for mobile data communication Approved 2007
- X.1124, Authentication architecture in mobile end-to-end data communication Approved 2007
- X.1125, Correlative reacting system in mobile network Approved 2007

Web Services security

- X.1143, Security architecture for message security in mobile Web Services, Approved 2007

Q9/17 Approved Recommendations

NID Security

- X.1171, Framework for Protection of Personally Identifiable Information in Networked ID Services.
  Consented 2008

Home network security

- X.1111, Framework for security technologies for home network, Approved 2007
- X.1112, Certificate profile for the device in the home network, Approved 2007
- X.1113, Guideline on user authentication mechanisms for home network service,
  Approved 2007

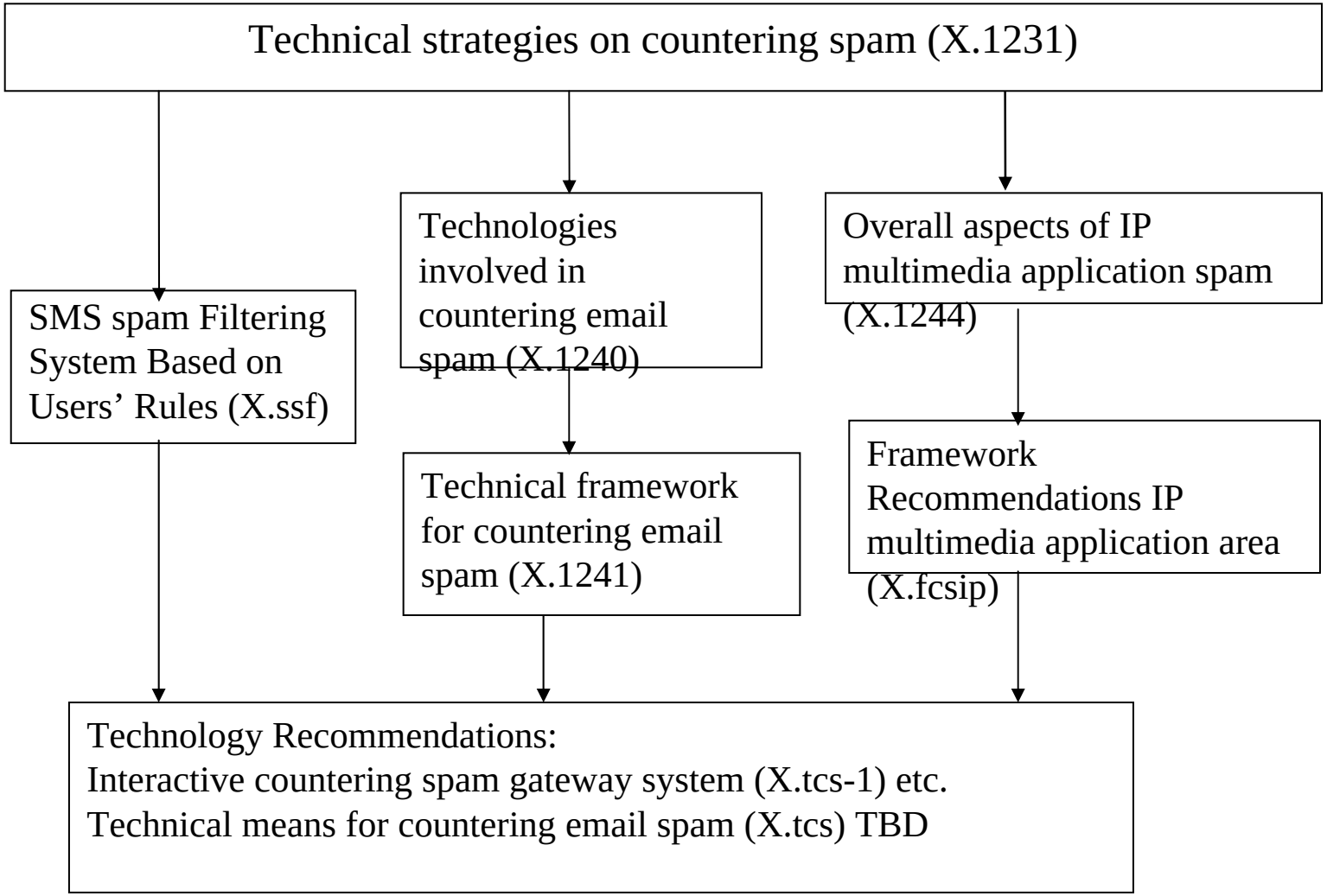
Secure applications services

- X.1151, Guideline on strong password authentication protocols,
  Approved 2007
- X.1152, Secure end-to-end data communication techniques using Trusted Third Party services, Consented 2008
- X.1161, Framework for secure peer-to-peer communications,
  Consented 2008
- X.1162, Security architecture and operations for peer-to-peer network,
  Consented 2008

Q.17/17: Combating spam by technical means

- Develops standards for countering spam by technical means, including:
  - General technical strategies and protocols for countering spam
  - Guidelines, frameworks and protocols for countering email spam, IP multimedia spam, SMS spam and other new types of spam

Q.17/17 strategic direction



Q17/17 Approved Recommendations

No.	Title
X.1231	Technical Strategies on Countering Spam
X.1240	Technologies involved in countering email spam
X.1241	Technical framework for countering email spam
X.1244*	Overall aspects of IP multimedia application spam

* Currently in approval process

SG 17 Security Recommendations under development

- Summaries of all Study Group 17 Recommendations under development are available on the Study Group 17 web page at:

  www.itu.int/itu-t/studygroups/com17

SG13 Q.15 – NGN Security

- All SG 13 Recommendations have a section on security
- Q15 aims to assure the security of the telecommunications infrastructure as PSTNs evolve to NGNs.
- Must address and develop network architectures that
  - Provide for maximal network and end-user resource protection
  - Allow for highly-distributed intelligence end-to-end
  - Allow for co-existence of multiple networking technologies
  - Provide for end-to-end security mechanisms
  - Provide for security solutions that apply over multiple administrative domains
- NGN security activities and Recommendations are listed under "Work Program"
  - **www.itu.int/itu-t/studygroups/com13/index.asp**

ITU-D Cybersecurity Activities

- ITU-D Study Group 1 Question 22/1: *Securing information and communication networks: Best practices for developing a culture of cybersecurity*
  - Developing a *Framework for Organizing National Cybersecurity Efforts*
- ITU-D Programme 3 *ITU Cybersecurity Work Programme to Assist Developing Countries.*
- *Cybersecurity Guide for Developing Countries (2006)*

SG17 Workshops

- New Horizons for Security Standardization
  - Held in Geneva 3-4 October 2005
  - Speakers, panelists, chairs from ATIS, ETSI, ITU, ISO/IEC, IETF, OASIS, RAIS , 3GPP
- Digital Identity for Next Generation Networks
  - Held in December 2006 jointly with ITU-T/EU IST Daidalos Project
- Conformance & Interoperability and Testing
  - Held in December 2006 to raise awareness of conformance and interoperability testing issues

International Telecommunication Union

Global Cybersecurity Agenda

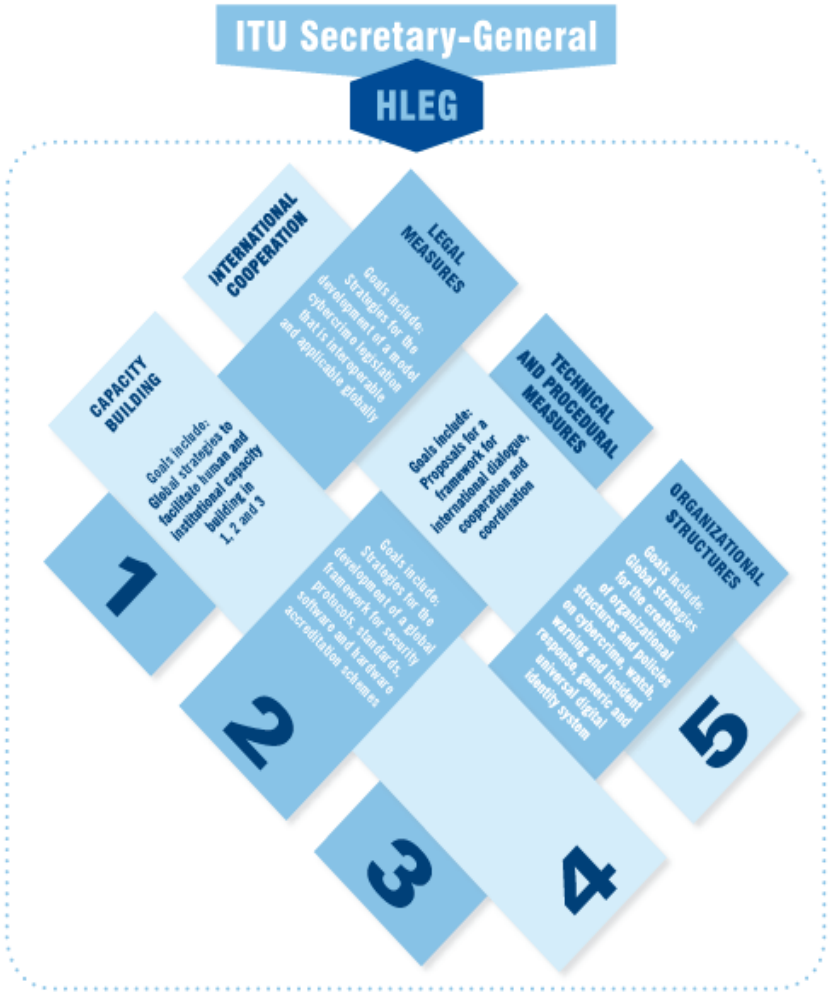
The strategy for a solution must identify those existing national, regional and international initiatives, work with all relevant players to identify priorities and bring partners together with the goal of proposing global solutions to address the global challenges we face today.

ITU Global Cybersecurity Agenda (GCA)

- A framework for international multi-stakeholder cooperation in cybersecurity
- ITU Response to its role as sole Facilitator for WSIS Action Line C5
- World renowned Group of High Level Experts (HLEG) to develop global strategies
- Representing main stakeholder groups working towards the same goals
- ***Developing harmonized global strategies***

GCA rests on five pillars or work areas:

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



High-Level Expert Group (HLEG)

A global multi-stakeholder think-tank made up of high-level experts from:

- Governments
- Industry
- Regional and international organizations
- Research and academic institutions
- Individual experts

provided advice on strategies in all five work areas or pillars

Elaboration of global strategies for

1 the development of a model cybercrime legislation

2 the creation of appropriate national and regional organizational structures and policies on cybercrime

3 the establishment of security criteria and accreditation schemes for software applications and systems

4 the creation of a global framework for watch, warning and incident response

5 the creation and endorsement of a generic and universal digital identity system

6 the facilitation of human and institutional capacity-building

7 international cooperation, dialogue and coordination

GCA/HLE Members

Argentina Brazil Cameroon Canada China Egypt Estonia Germany Japan India Indonesia Italy Malaysia Morocco Portugal Republic of Lithuania Russian Federation Saudi Arabia South Africa Switzerland United States

Diversity of Participation

- Ecole Polytechnique Fédérale de Lausanne (EPFL), Switzerland
- Information Security Institute, Australia
- Moscow Technical University of Communications, Russian Federation
- African Telecommunication Union (ATU)
- Asia Pacific Economic Cooperation
- Telecommunications (APECTEL)
- Commonwealth Telecommunications Organisations (CTO)
- Council of Europe
- Department of Economic and Social Affairs (DESA)
- European Information and Network
- Security Agency (ENISA)
- International Criminal Police Organization (Interpol)
- Organisation for Economic Co-operation and Development (OECD)
- Organisation International de la Francophonie
- Society for the Policing of Cyberspace (POLCYB)
- UMTS Forum
- United Nations Institute for Training and Research (UNITAR)
- United Nations Office on Drugs and Crime

- Authentrus
- BITEK International Inc.
- Cybex
- Cisco
- Garlik
- Intel Corporation
- Microsoft Corporation
- Télam S.E.
- VeriSign, Inc.
- Stein Schjolberg, Chief Judge, Moss Tingrett Court, Norway
- Solange Ghernaouti-Helie, HEC-Université de Lausanne, Switzerland
- Sy Goodman, Georgia Institute of Technology, United States
- Nabil Kisrawi, Chairman of WG-Def, Syrian Republic
- Bruce Schneier, Security Technologist, Unites States
- Marco Gercke, Professor, Cologne University, Germany

HLEG

- The HLEG work is an ongoing dynamic process with information-sharing and interaction relating to the elaboration of Global Strategies to meet the goals of the GCA and the ITU role as sole facilitator for WSIS Action Line C.5.

- Three meetings held:
  - First Meeting of the HLEG held on 5 October 2007
  - Second Meeting of the HLEG held on 21 May 2008
  - Third Meeting of the HLEG held on 26 June 2008

- Chairman's Report:
  - The results of the work of the HLEG, including recommendations, the views expressed during the meeting and additional information about the previous work of the HLEG are contained in the Chairman's report which will be available at: http://www.itu.int/osg/csd/cybersecurity/gca/hleg/meetings/third/index.html

For More information on:

ITU Global Cybersecurity Agenda & ITU Activities in Cybersecurity:

www.itu.int/cybersecurity/

Email: gca@itu.int

International Telecommunication Union

A look at some specific SG 17 security projects and outreach activities

Focus Group: Security Baseline for Network Operators

- Established October 2005 by SG 17
- Objectives:
  - Define a security baseline against which network operators can assess their network and information security posture in terms of what security standards are available, which of these standards should be used to meet particular requirements, when they should be used, and how they should be applied
  - Describe a network operator's readiness and ability to collaborate with other entities (operators, users and law enforcement authorities) to counteract information security threats
  - Provide meaningful criteria that can be used by network operators against which other network operators can be assessed, if required.
- Survey network operators and service providers conducted in November 2006 by means of a questionnaire
- In September 2007 the resulting security baseline was approved as a Supplement to X.800 series standards

ITU-T

Security Manual

- *Security in Telecommunications and Information Technology* – an overview of existing ITU-T recommendations for secure telecommunications.
- Available in hard copy and on the SG 17 part of the ITU-T publications web site at
- Will be updated later this year
- www.itu.int/publications

Security compendium

- Catalogue of approved ITU-T Recommendations related to telecommunication security
  - Summary of ITU-T Study Groups with security-related activities
  - Extract of ITU-T approved security definitions
  - **http://www.itu.int/ITU-T/studygroups/com17/tel-security.html**

ITU-T

Security Standards Roadmap

- An on-line security standards resource.
- In collaboration with ENISA and NISSG
- Comprises 5 parts:
  - Part 1 contains information about organizations working on ICT security standards
  - Part 2 is database of existing security standards
  - Part 3 lists (or links to) current projects and standards in development
  - Part 4 identifies future needs and proposed new standards
  - Part 5 lists security best practices

Roadmap - 2

ITU-T

- Part 2 is a searchable database that includes ITU-T, ISO/IEC JTC1, IETF, ATIS, ETSI, IEEE, 3GPP and OASIS security standards.
- The database format allows searching and to allows organizations to manage their own data
- Publicly available under *Special Projects and Issues* at:
  - www.itu.int/ITU-T/studygroups/com17/index
- We invite you to use the Roadmap, provide feedback and help us develop it to meet your needs

Some closing thoughts

The importance of Collaboration

- Internal and external collaboration is very important to the work of SG17
- Examples include:
  - Most other ITU-T SGs, ITU-D, ISO/IEC JTC1, IETF, ATIS, ETSI, OASIS etc
  - ENISA, NISSG (Roadmap)
  - Global Standards Collaboration (GSC)
  - ISO/IEC/ITU-T Strategic Advisory Group on Security (SAG-S)

ITU-T

Summary

- ITU-T security work is producing solid results to address current and emerging threats
- Threats are not going to diminish. We need to continue to focus on the security issue when developing all new ICT standards
- It is very important that we continue to work in concert with other SDOs and agencies with an interest in ICT security

Some useful web resources

- ITU-T Home page http://www.itu.int/ITU-T/
- Study Group 17 http://www.itu.int/ITU-T/studygroups/com17/index.asp
  e-mail: tsbsg17@itu.int
- LSG on Security http://www.itu.int/ITU-T/studygroups/com17/tel-security.html
- Security Roadmap http://www.itu.int/ITU-T/studygroups/com17/ict/index.html
- Security Manual http://www.itu.int/publ/T-HDB-SEC.03-2006/en
- Cybersecurity Portal http://www.itu.int/cybersecurity/
- Cybersecurity Gateway http://www.itu.int/cybersecurity/gateway/index.html
- Recommendations http://www.itu.int/ITU-T/publications/recs.html
- ITU-T Lighthouse http://www.itu.int/ITU-T/lighthouse/index.phtml
- ITU-T Workshops http://www.itu.int/ITU-T/worksem/index.html

Thank You