Asia-Pacific Forum on
Bridging Standardization Gap
Ha Noi, Viet Nam, 15 – 17 September 2008

Cybersecurity: a challenge for the ITU

Paolo Rosa

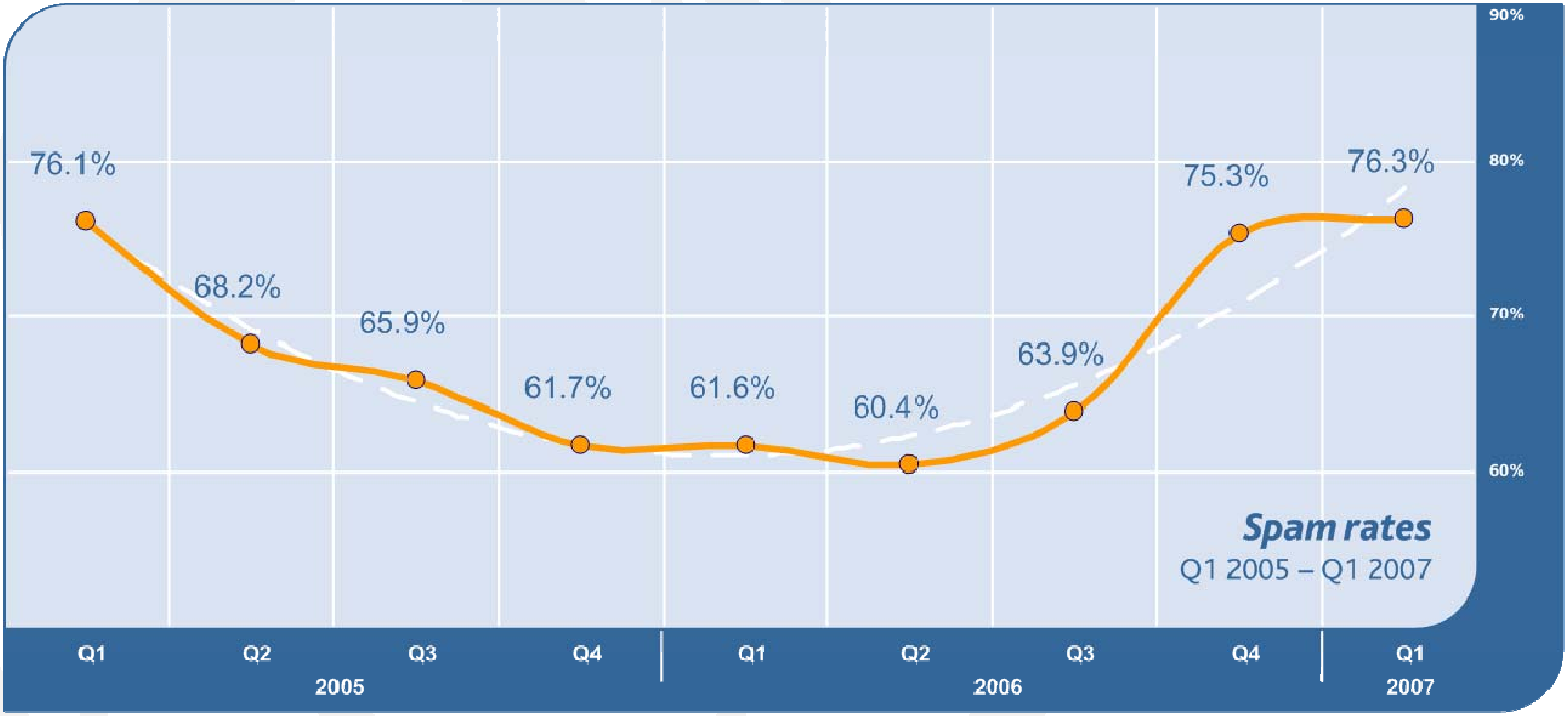
Head, Workshops and Promotion Division
ITU - Telecommunication
Standardization
Bureau

The issue

- Security is **everybody's business and requires** Collaboration with other SDOs
- Security needs to be **designed in upfront**
- Security must be an **ongoing effort**
- Systematically addressing **vulnerabilities** (intrinsic properties of networks/systems) is key so that protection can be provided independent of what the **threats** (which are constantly changing and may be unknown) may be

Committed to connecting the world

Combatting spam: Current threat level
Spam as a % of all email, worldwide



Source: MessageLabs.

International Telecommunication Union

Committed to connecting the world

PP-06 Resolutions related to security

- Resolution 130: Strengthening ITU’s role in building confidence and trust in use of ICTs
  - – Resolves to give this work a high priority in ITU
  - – Requests a review of current work and progress
  - – Instructs to facilitate access to tools and to continue cybersecurity gateway
- Resolution 149: Study of definitions and terminology relating to Res 130
  - – Establishes a working group (chair: Nabil Kisrawi, Syrian Arab Republic)
  - – Report to PP-2010

International Telecommunication Union

Committed to connecting the world

WTSA-04 Resolutions related to cybersecurity and combatting spam

- Res. 50: Cybersecurity
  - Calls on ITU-T to evaluate Recs with respect to cybersecurity threats and to raise awareness
- Res. 51: Combating spam
  - Calls on the ITU-T Director to report to Council on relevant initiatives for combating spam
- Res. 52: Countering spam by technical means
  - Instructs relevant Study Groups, in collaboration with IETF, to develop technical Recs, including definitions, on countering spam

Outline

- Cybersecurity and Cyberspace
- World Summit on Information Society
- ITU Activities on Cyber security
- ITU-T (standards) activities
- ITU-D (development) activities

International Telecommunication Union

Committed to connecting the world

Cybersecurity & Cyberspace

Draft new ITU-T Rec.X1205
Overview of Cybersecurity

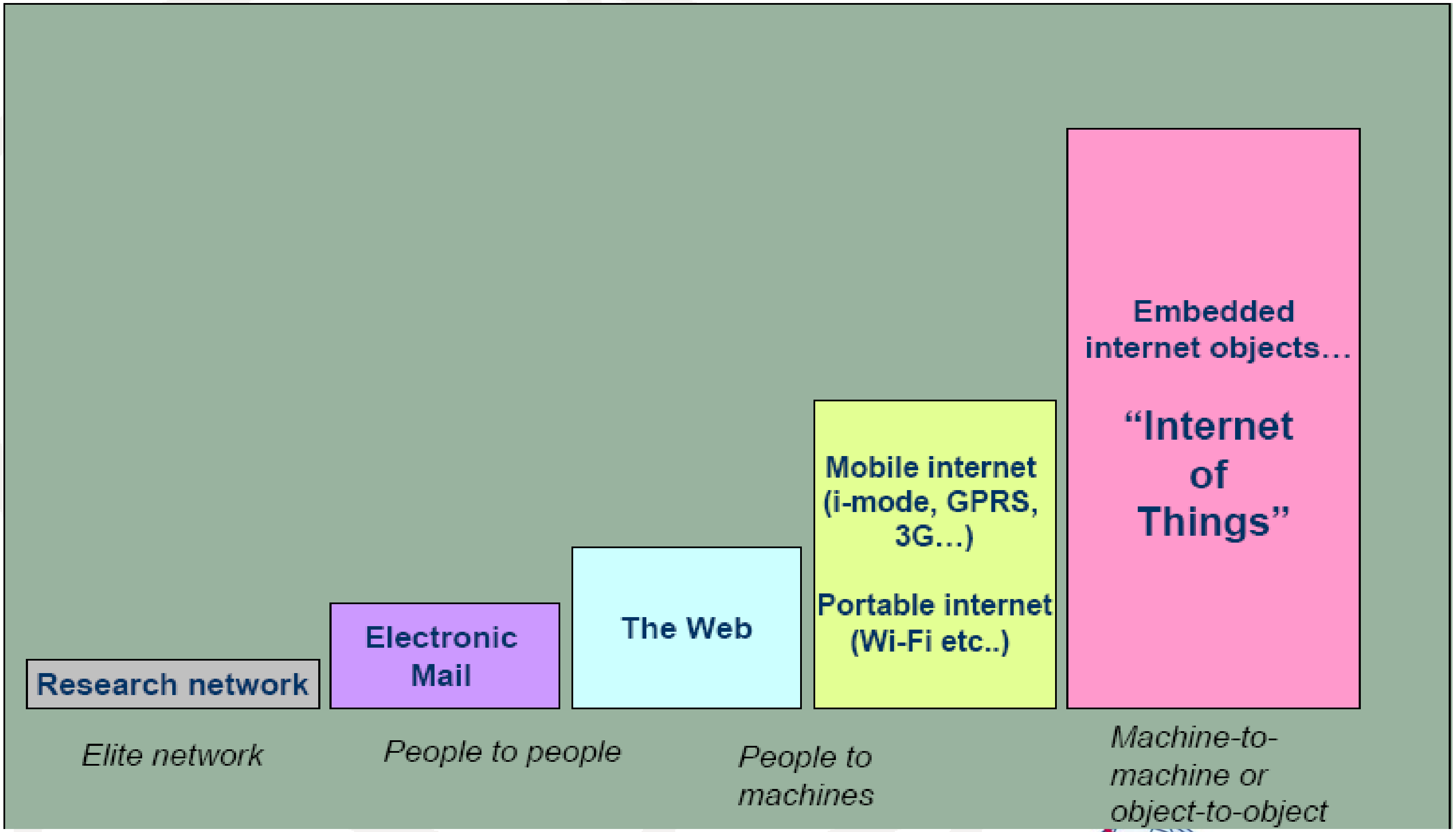
- **Cybersecurity:** collection of tools, policies, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the **cyberspace** against relevant security risks such as unauthorized access, modification, theft, disruption, or other threats

- **Cyberspace:** the cyber environment including software, connected computing devices, computing users, applications/services, communications systems, multimedia communication, and the totality of transmitted and/or stored information connected directly or indirectly to the Internet. It includes hosting infrastructures and isolated devices

International Telecommunication Union

Committed to connecting the world

Changing nature of cyberspace



Research network

Electronic Mail

The Web

Mobile internet (i-mode, GPRS, 3G…)

Portable internet (Wi-Fi etc..)

Embedded internet objects…

"Internet of Things"

Elite network

People to people

People to machines

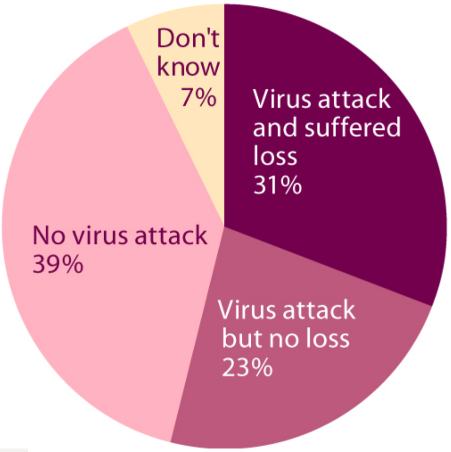
Machine-to-machine or object-to-object

Source: Presentation materials at ITU workshop on "Ubiquitous Network Societies", April 2005.

Threats in cyberspace

- **Inherited architecture of the Internet was not designed to optimize security**
- Constant evolution of the nature of cyberthreats
- Low entry barriers and increasing sophistication of cybercrime
- Constant evolution in protocols and algorithms
- Loopholes in current legal frameworks
- Introduction of Next-Generation Networks (NGN)
- Convergence among ICT services and networks
- Network effects – risks far greater
- Possibility of anonymity on the Internet
- Absence of appropriate organizational structures
- Internationalization requires cross-border cooperation
- Vulnerabilities of software applications

Proportion of home users in Singapore that had experienced a virus attack, 2006



International Telecommunication Union

Committed to connecting the world

Attackers, hackers and intruders

(generally users cannot be trusted)

- Taxonomy of security threats
  - **Unauthorized illegal access**: insufficient security measures autent./author/unprotected passwords…
  - **IP spoofing**: assume a trusted host identity, disable host, assume attacker's identity, access to IP addresses)
  - **Network sniffers**: read source and destination addresses, passwords,data…
  - **Denial of Service** (DoS): connectivity, network elements or applications availability
  - **Bucket brigade attacks**: messages interception/modification
  - **Back door traps**: placed by system developers / employees /operating system/created by virus
  - **Masquerading**: access to the network as false legitimate personnel
  - **Reply attacks**: read authentication information from messages
  - **Modification of messages** without detection
  - **Insider attacks:** legitimate users behave in unauthorized way, needed perdiodical auditing actions, screening of personnel, hardware and software

International Telecommunication Union

Committed to connecting the world

Challenges: Policy

- Lack of relevant cybercrime and anti-spam legislation
  - Establish where none
    - Base “model law” needed (which is separate ITU initiative)
  - Modify existing cybercrime/spam laws where needed to reflect botnet-related crime

- Capacity building for regulators, police, judiciary
  - Training existing officials may be supplemented by co-opting or active recruitment of technical experts

- Weak international cooperation and outreach
  - Participation in local, regional and international initiatives
  - Engagement of relevant government, regulators, law enforcement with peers and other stakeholders around globe
  - Targeted outreach to countries and stakeholders known to be particularly vulnerable to cybercrime

ITU Cybersecurity activities

WSIS Action Line C.5

Building Confidence and security in the use of ICTs

http://www.itu.int/wsis/c5/index.html

ITU Global Cybersecurity Agenda

Framework for international cooperation in Cybersecurity

CYBERSECURITY GATEWAY

Welcome to the Cybersecurity Gateway!

WSIS Action Line C5 Facilitation

ITU Cybersecurity Gateway

Information resource on Cybersecurity

International Telecommunication Union

Committed to connecting the world

WSIS

world summit
on the information society
Geneva 2003 - Tunis 2005

ITU International Telecommunication Union
Committed to connecting the world

Main issues from WSIS – C5

- Critical information infrastructure protection (CIIP);
- Promotion of a global culture of cybersecurity;
- Harmonizing national legal approaches, intl. legal coordination & enforcement;
- Countering spam;
- Developing watch, warning and incident response capabilities;
- Information sharing of national approaches, good practices and guidelines;
- Privacy, data and consumer protection.
- http://www.itu.int/osg/spu/cybersecurity/pgc/background.phtml

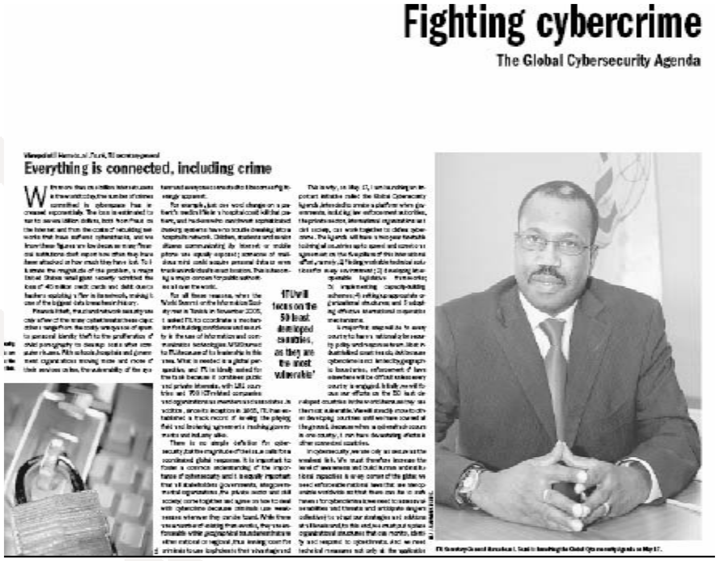
ITU International Telecommunication Union

Committed to connecting the world

ITU activities on Cybersecurity

The Global Cybersecurity Agenda

- Launched in May 2007 by the ITU’s Secretary-General, Dr. Hamadoun Touré on World Telecommunication and Information Society Day
- The Global Cybersecurity Agenda (GCA): a ITU framework for international cooperation aimed at proposing strategies for solutions to enhance confidence and security in the use of ICTs
- will build on existing national and regional initiatives
- avoid duplication and encourage collaboration



Fighting cybercrime

The Global Cybersecurity Agenda

Everything is connected, including crime

[illegible]

'ITU will focus on the 50 least developed countries, as they are the most vulnerable'

17 May 2007, International Herald Tribune

9 July 2007, UN Secretary-General historic visit to ITU

ITU GCA main goals

Elaboration of strategies to:

- develop a model **cybercrime legislation** globally applicable, interoperable with existing national / regional legislative measures
- create national and regional **organizational structures and policies on cybercrime**
- establish globally accepted minimum **security criteria and accreditation schemes for software applications and systems**
- create a **global framework for watch, warning and incident response** to ensure cross-border coordination of initiatives
- create and endorse a **generic and universal digital identity system** and the necessary organizational structures to ensure the recognition of digital credentials for individuals across geographical boundaries
- develop a *global strategy to facilitate* **human and institutional capacity-building** to enhance knowledge and know-how across sectors and in all the above-mentioned areas
- advice on potential framework for a *global multi-stakeholder strategy for* **international cooperation, dialogue and coordination** in all the above-mentioned areas.

The High Level Segment

- Held on the opening of the ITU council meetings
- Participation of Ministers
- Questions addressed:
  - Greatest cyberthreats faced worldwide
  - Key elements to formulate national strategies and to prevent cybercrime
  - Role of governments in promoting a cibersecurity culture
  - Highest priority activities to address current and emerging cyberthreats

International Telecommunication Union

Committed to connecting the world

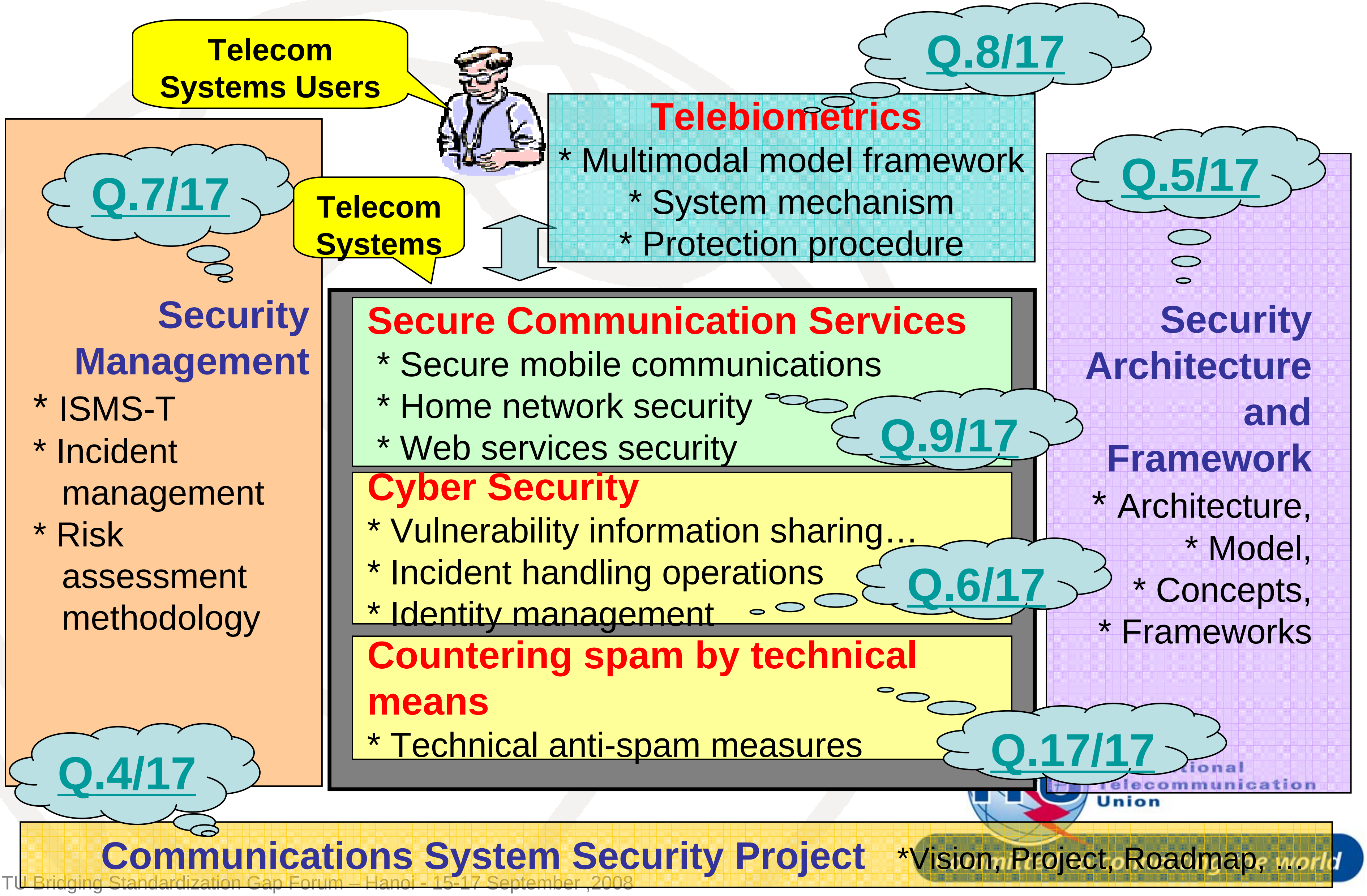
ITU-T standardization activities on security

(focus on ITU-T Study Group 17)

International Telecommunication Union

Committed to connecting the world

SG 17: Security Questions



Telecom Systems Users

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.4/17

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.5/17

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

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

ITU-T Security Building Blocks

Security Architecture Framework (X.800-series)

Network Management Security (M.3000-series)

Security Techniques (X.841,2,3)

New
Telecommunication Security (X.805, X.1000-series)

Systems Management (X.733,5,6, X.740,1)

Protocols (X.273,4)

Facsimile (T-series)

New
NGN Security (Y.2700-series)

Directory Services and Authentication (X.500-series)

Televisions and Cable Systems (J-series)

Security in Frame Relay (X.272)

Message Handling Systems (MHS) (X.400-series)

Multimedia Communications (H-series)

End-to-end communication security ITU-T Rec.X.805 and draft Rec.X.1205

- **Security dimensions**
  - Access control;
  - Authentication;
  - Non-repudiation;
  - Data confidentiality;
  - Communication security;
  - Data integrity;
  - Availability; and
  - Privacy.
- **Security layers**
  - Infrastructure;
  - Services;
  - Applications;
- **Security planes** (network activity protected by security dimensions)
  - Management;
  - Control;
  - End user;
- **Cybersecurity technologies**
  - Cryptography
  - Access control;
  - System integrity;
  - Audit, logging & monitoring;
  - Management;

Identity Management

- **Management of digital identity**
  - All trusted ICT and network capabilities and resources for
    - Authentication (e.g., certificates)
    - Identifiers (e.g., E.164 nos., URIs, IP addresses, domain names)
    - Attributes (e.g., names, location)
    - Patterns and reputation
  - For entities of any kind
    - People
    - Organizations
    - Objects (e.g., devices, SIMs, RFIDs, content..)
- **Common global needs for interoperability**
  - Essential for network/cybersecurity and eCommerce
  - Essential for an increasingly “always on” world

Focus Group on Identity Management

- Created in December 2006, by TSAG
- Six meetings in Geneva (x3), Mountain View, Tokyo and Cambridge; workshop in Lucerne
- Focus Group products
  - Requirements structure and provisions
  - Use cases, platforms, gaps
  - Draft framework(s)
  - Reference materials, including a lexicon and a legal/regulatory compendium
- Inputs to Study Groups 13 and 17

International Telecommunication Union

Committed to connecting the world

ICT security standards roadmap

- **Part 1** contains information about organizations working on ICT security standards
- **Part 2** is database of existing security standards and includes ITU-T, ISO/IEC JTC 1,IETF, IEEE, ATIS, ETSI and OASIS security standards
- **Part 3** is a list of standards in development
- **Part 4** identifies future needs and proposed new standards
- **Part 5** includes Security Best Practices

http://www.itu.int/ITU-T/studygroups/com17/ict/

International Telecommunication Union

Committed to connecting the world

ITU-D cybersecurity activities

Committed to connecting the world

Countering Spam and Related Threats

- Survey on Anti-Spam Legislation Worldwide
- Botnet Mitigation Toolkit for Developing Countries
  - Pilot Projects for Implementation of Toolkit (Malaysia, India)

- Joint Activities for StopSpamAlliance.org
- Study on Economics of Spam (with ITU-T Study Group 3)
- Translation of Message Anti-Abuse Working Group Best Practices Docs
  - Code of Conduct
  - MAAWG -Managing Port25
  - BIAC-MAAWG Best Practices Expansion Document
  - Anti-Phishing Best Practices for ISPs and Mailbox Providers
  - MAAWG Sender BCP Version 1.1& Executive Summary
- References
  - http://www.itu.int/ITU-D/cyb/cybersecurity/spam.html
  - http://www.itu.int/ITU-D/cyb/cybersecurity/projects/botnet.html

International Telecommunication Union

Committed to connecting the world

ITU Cybersecurity Work Programme to Assist Developing Countries

- Most countries have not formulated or implemented a national strategy for cybersecurity and Critical Information Infrastructure Protection (CIIP)
- ITU Work Programme scopes a set of proposed high level assistance activities
- Contains set of detailed initiatives planned in the 2007- 2009 period by the *ITU Development Sector's ICT Applications and Cybersecurity Division*

ITU Cybersecurity Work Programme
to Assist Developing Countries
2007-2009

ICT Applications and Cybersecurity Division
Policies and Strategies Department
ITU Telecommunication Development Bureau

20 June 2007 DRAFT

Please send comments to cybmail@itu.int

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

International
Telecommunication
Union

Committed to connecting the world

ITU National Cybersecurity/CIIP Self–Assessment Toolkit

- Includes Annex on *Deterring Cybercrime: Substantive, Procedural and Mutual Assistance Law Baseline Survey*
- Intended to assist national authorities to review their domestic situation related to goals and actions identified in:
  - UN Resolutions 55/63(2000) and 56/121(2001): Combating the Criminal Misuse of Information Technologies
  - Council of Europe’s Convention on Cybercrime(2001)
- Adopted from work in APEC-TEL

ITU National Cybersecurity/CIIP
Self-Assessment Toolkit

[illegible]

International Telecommunication Union

Committed to connecting the world

Information Sharing through Enhancing the ITU Cybersecurity Gateway

Establishment of an ITU Cybersecurity/CIIP Directory
Establishment of an ITU Cybersecurity/CIIP Contact Database
Establishment of Annual Who's Who in Cybersecurity/CIIP Publication
Establishment of an Annual ITU Cybersecurity Publication
ITU Cybersecurity Fellowship Programme for Developing Countries

- Enhancement of the ITU Cybersecurity GatewayIntegration with ICT Eye?
- Integration with Microsoft Virtual Earth or Google Earth

Referenceshttp://www.itu.int/cybersecurity/gateway/

International Telecommunication Union
Committed to connecting the world

Establishment of National Strategies/Capabilities for Cybersecurity and Critical Information Infrastructure Protection (CIIP)

- Identification of Best Practices in the Establishment of National Frameworks for Cybersecurity and CIIP
- National Cybersecurity/CIIP Readiness Self-Assessment ToolkitPilot tests in selected countries
- Regional Workshops on Frameworks for Cybersecurity and CIIP
- Online Cybersecurity Experts Forum to Help Developing Countries Develop Capacity
- Toolkit for Promoting a Culture of Cybersecurity
- Online Training Modules for Cybersecurity Awareness and Solutions

References:

http://www.itu.int/ITU-D/cyb/cybersecurity/projects/readiness.html
http://www.itu.int/ITU-D/cyb/cybersecurity/strategies.html
http://www.itu.int/ITU-D/cyb/events/

International Telecommunication Union

Committed to connecting the world

Establishment of Appropriate Cybercrime Legislation and Enforcement Mechanisms

- Regional Capacity Building Activities on Cybercrime Legislation and Enforcement
- Publication: Understanding Cybercrime: A Guide for Developing Countries (end 2007)
- Model Cybercrime Law Project (early 2008)

- Cybersecurity Module in the ITU/InfoDev ICT Regulation Toolkit

References: http://www.itu.int/ITU-D/cyb/cybersecurity/legislation.html

Establishment of Watch, Warning and Incident Response (WWIR) Capabilities

- Assistance to Developing Countries related to Establishment of Watch, Warning and Incident Response (WWIR) Capabilities
- Inventory of Watch, Warning and Incident Response Capabilities by Region
- Standard Reporting Format for Fraudulent Online Activities

References: www.itu.int/ITU-D/cyb/cybersecurity/wwir.html

International Telecommunication Union

Committed to connecting the world

Cybersecurity Gateway

- Provides an easy-to-use information resource on national and international cybersecurity related initiatives worldwide
- Separate portals for:
  - Citizens
  - Governments
  - Businesses
  - International organizations
- Interactive map for country-speci
- www.itu.int/cybersecurity/gateway

CYBERSECURITY GATEWAY
Welcome to the Cybersecurity Gateway!
Information Sharing
Watch and Warning
Industry Standards and Solutions
Laws and Legislation
Privacy and Protection
WSIS Action Line C5 Implementation
Cybersecurity and Developing Economies

International Telecommunication Union

Committed to connecting the world

Information Sharing through Enhancing the ITU Cybersecurity Gateway

Establishment of an ITU Cybersecurity/CIIP Directory
Establishment of an ITU Cybersecurity/CIIP Contact Database
Establishment of Annual Who's Who in Cybersecurity/CIIP Publication
Establishment of an Annual ITU Cybersecurity Publication
ITU Cybersecurity Fellowship Programme for Developing Countries

Enhancement of the ITU Cybersecurity GatewayIntegration with ICT Eye?
Integration with Microsoft Virtual Earth or Google Earth

Referenceshttp://www.itu.int/cybersecurity/gateway/

International Telecommunication Union
Committed to connecting the world

Thank you

ITU

Committed to Connecting the World

Paolo ROSA
tsbpromo@itu.int

International
Telecommunication
Union

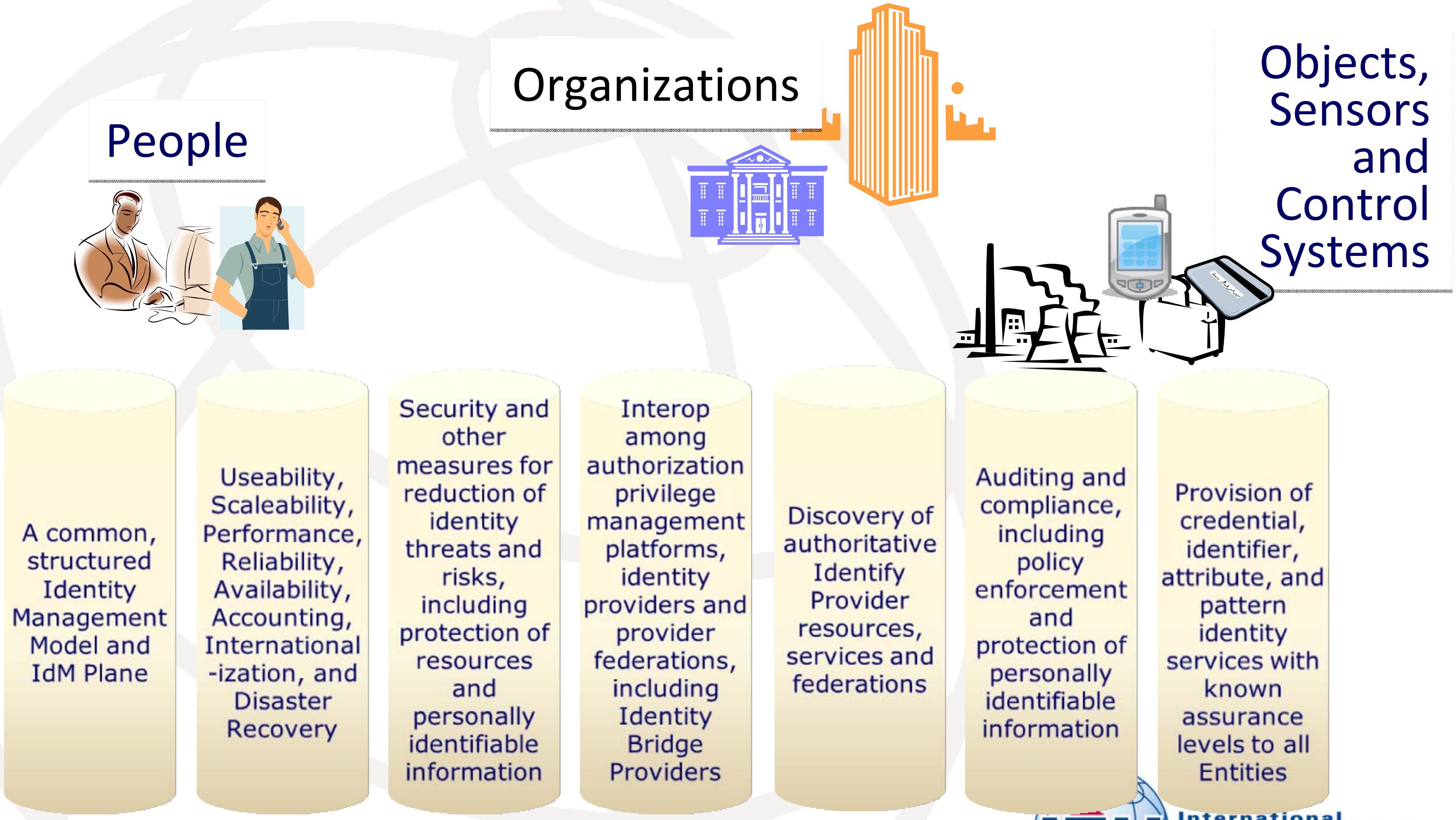
Committed to connecting the world

Additional Slides

International Telecommunication Union

Committed to connecting the world

The “seven pillars” for globally interoperable Identity Management



People

Organizations

Objects, Sensors and Control Systems

A common, structured Identity Management Model and IdM Plane

Useability, Scaleability, Performance, Reliability, Availability, Accounting, International-ization, and Disaster Recovery

Security and other measures for reduction of identity threats and risks, including protection of resources and personally identifiable information

Interop among authorization privilege management platforms, identity providers and provider federations, including Identity Bridge Providers

Discovery of authoritative Identify Provider resources, services and federations

Auditing and compliance, including policy enforcement and protection of personally identifiable information

Provision of credential, identifier, attribute, and pattern identity services with known assurance levels to all Entities

International Telecommunication Union

Committed to connecting the world

Source: Rutkowski, ITU-T Focus Group on IdM.

Some useful security web resources

- **ITU-T Home page**: www.itu.int/ITU-T
- **Study Group 17**:

  www.itu.int/ITUT/studygroups/com17

  e-mail: tsbsg17@itu.int
- **Recommendations**:

  www.itu.int/ITU-T/publications/recs.html
- **ITU-T Lighthouse**: www.itu.int/ITU-T/lighthouse
- **ITU-T Workshops**: www.itu.int/ITU-T/worksem
- **Security Roadmap**:

  www.itu.int/ITU-T/studygroups/com17/index

International Telecommunication Union

Committed to connecting the world