2009 ITU Regional Cybersecurity Forum for Americas

Santo Domingo, Dominican Republic
23-25 November 2009

Cybersecurity, ITU-T standards and initiatives

Georges Sebek
Counsellor
ITU/TSB

Building confidence and security in the use of Information and Communication Technologies (ICTs) is one of the most important, and most complex, challenges we face today.

Promoting cybersecurity is a top priority, if we are to reap the full benefits of the digital revolution and the new and evolving communication technologies coming onto the market.

At the same time, maintaining cybersecurity is a culture, spanning different disciplines, that needs to be built into our approach towards, and our adoption of, these new technologies.

ITU, with its tradition as an international forum for cooperation and its important work in technical standards for security, has a vital contribution to make in promoting cybersecurity. ITU can draw on its expertise in standardization as well as its experience in direct technical assistance to members, to build a multi-disciplinary approach towards maintaining cybersecurity.

It has never been more important for those that seek to defend the safety, security and integrity of the world's ICT networks to step up their efforts.

An important part of this process is standardization work, to ensure that common standards for network security are adopted as widely as possible.

Not only will harmonization of standards increase the level of security, it will also reduce the costs of building secure systems.

ITU-T Study Group 17 has the lead responsibility for security

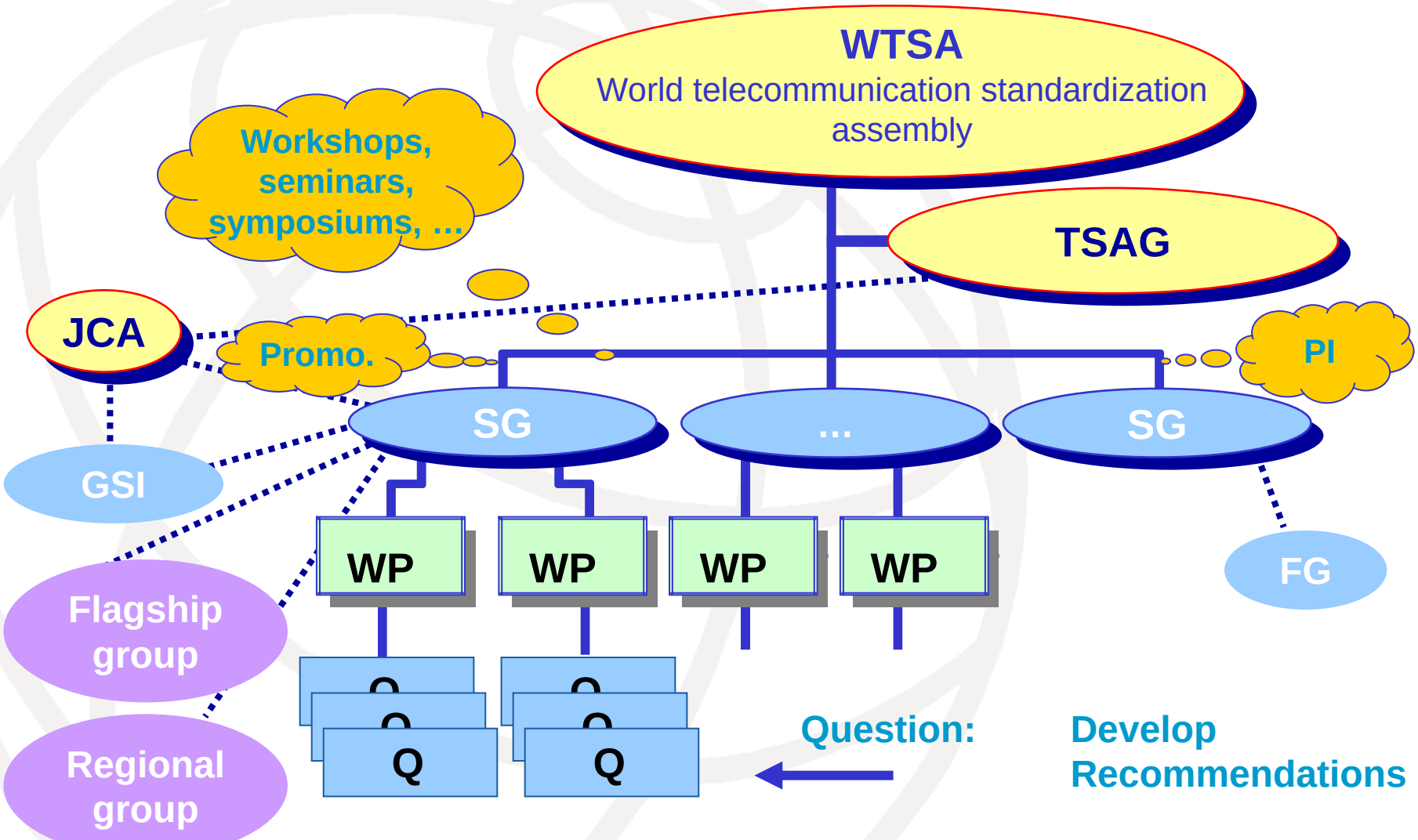
Cybersecurity

- ITU-T X.1205, *Overview of cybersecurity*
  - Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following:
    - Availability
    - Integrity, which may include authenticity and non-repudiation
    - Confidentiality

Strategic context

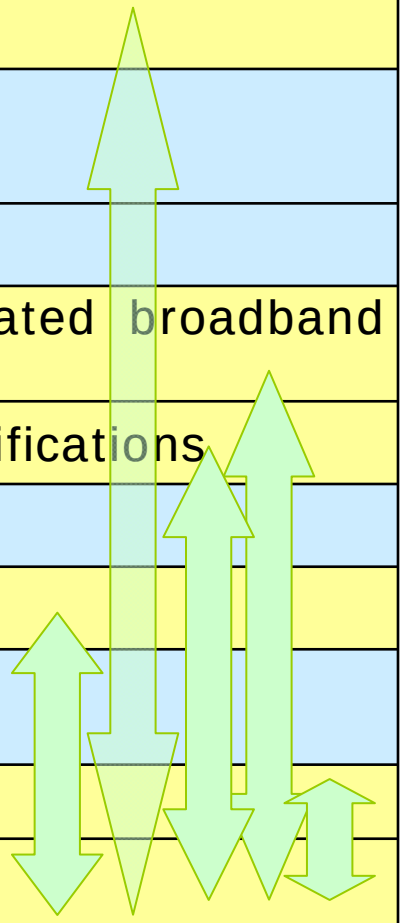
- **WSIS Action Line C5**, Building confidence and security in use of ICTs
- **PP-06 Resolution 130**, Strengthening the role of ITU in building confidence and security in the use of information and communication technologies
  - Director of TSB to develop projects for enhancing cooperation on cybersecurity and combating spam responding to the needs of developing countries
- **PP-06 Resolution 149**, Study of definitions and terminology relating to building confidence and security in the use of information and communication technologies
  - To establish a WG of the Council to study terminology re. building confidence and security in use of ICTs
- **WTSA-08 Resolutions 2, 50, 52, 58, 76**
  - Mandate for ITU-T SG 17, cybersecurity, countering and combatting spam, encourage the creation of national CIRTs, particularly for developing countries, studies relating to conformance and interoperability testing, assistance to developing countries, and a future possible ITU Mark programme

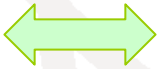
ITU-T Structure



ITU-T study groups for study period 2009-2012

SG 2	Operational aspects of service provision and telecommunications management
SG 3	Tariff & accounting principles including related telecommunication economic & policy issues
SG 5	Environment and climate change
SG 9	Television and sound transmission and integrated broadband cable networks
SG 11	Signalling requirements, protocols and test specifications
SG 12	Performance, QoS and QoE
SG 13	Future networks including mobile and NGN
SG 15	Optical transport networks and access network infrastructures
SG 16	Multimedia coding, systems and applications
SG 17	**Security**



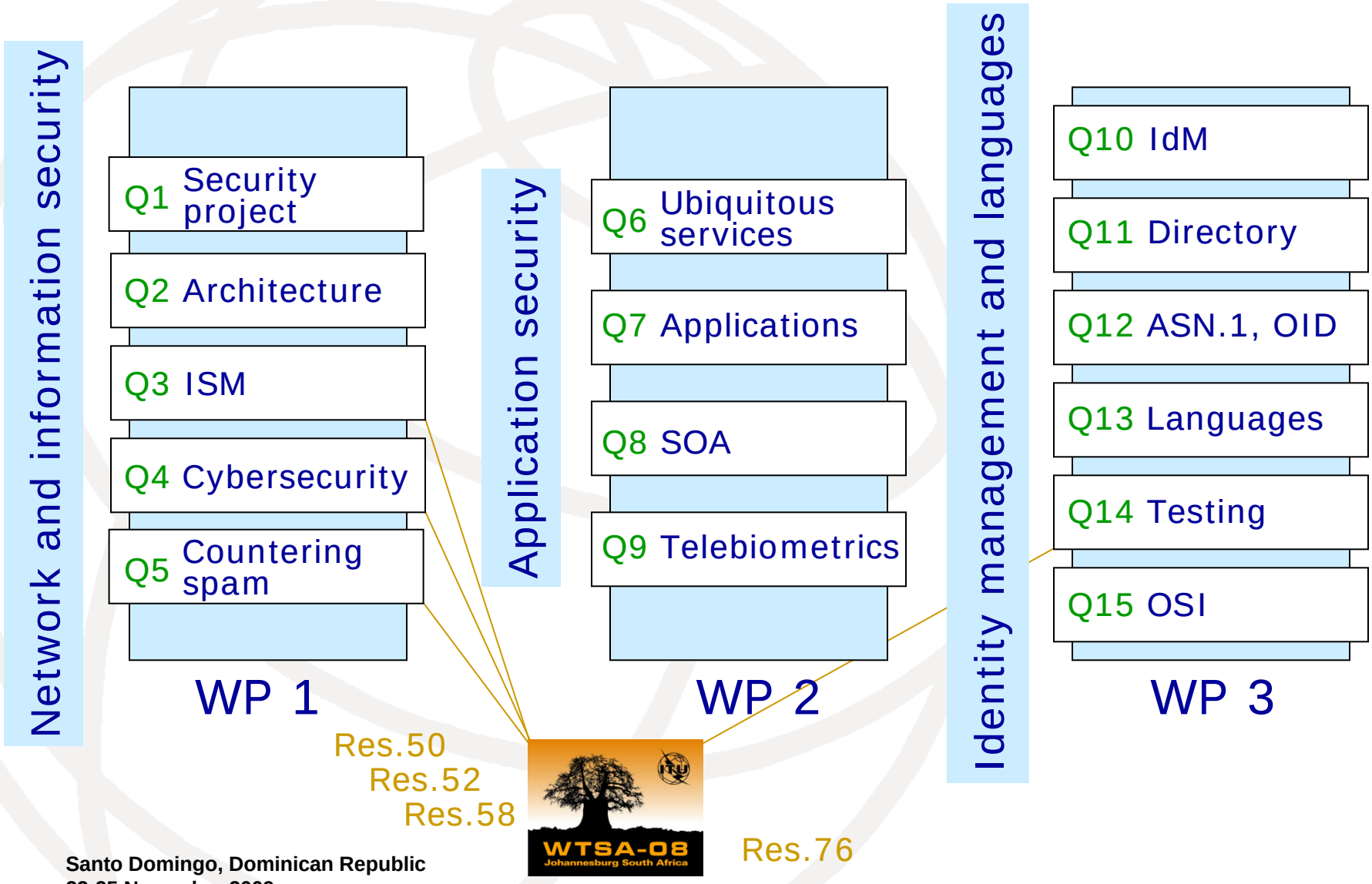


Relationships

ITU-T SG 17 role and mandate

- Responsible for studies relating to security including cybersecurity, countering spam and identity management. Also responsible for the application of open system communications including directory [X.509] and object identifiers, and for technical languages, the method for their usage and other issues related to the software aspects of telecommunication systems.
- Lead study group on telecommunication security, identity management (IdM) and languages and description techniques

SG 17 structure



Core security Recommendations

- **Strong ramp-up on developing core security Recommendations in SG 17**
  - 24 approved in 2007
  - 36 approved in 2008
  - 100+ under development for approval this study period
- **Subjects include:**
  - Architecture and frameworks • Web Services • Directory • Identity management • Risk management • Cybersecurity • Incident management • Mobile security • Countering spam • Information security management • Secure applications • Telebiometrics • Ubiquitous telecommunication services • IPTV
- **Ramping up on:**
  - Traceback • Ubiquitous sensor networks • SOA • Privacy • Global cybersecurity information exchange framework (CYBEX)
- **Collaboration with others on many items**

Some SG 17 security projects and initiatives

ITU-T security project

Q.1/17

- **Security Coordination**
  - Coordinate within SG 17, with ITU-T SGs, with ITU-D and externally
  - Keep others informed - TSAG, IGF, ISO/IEC/ITU-T SAG-S...
  - Participate in workshops/seminars and to GSC
  - Maintain reference information on LSG security webpage
- **Security Compendium**
  - Regularly update the catalogue of approved security-related Recommendations and security definitions extracted from those approved Recommendations
- **ICT Security Standards Roadmap**
  - Keep updated the searchable database of approved ICT security standards from ITU-T and others (e.g., ISO/IEC, IETF, ETSI, IEEE, ATIS)
- **ITU-T Security Manual** (4th edition planned 4Q/2009)
- **Business use of telecommunication/ICT security standards** (new initiative)

Needs of developing countries for the reduction of the ICT security standardization gap

Q.1/17

- Study carried out by SG 17 from May 2008
  - The overall level of concern about cyber security in the responding administrations of the DCs/CETs is high
  - There is a high level of interest in the possibility of obtaining advice and/or assistance on ICT security from the ITU
  - The ITU needs to do better in promoting its ICT security products to the DCs/CETs
  - Awareness of the importance of the Directory (X.509) to ICT security is relatively low
    - Most responding administrations from DCs/CETs have not assessed their Directory needs regarding cybersecurity
- Eight recommendations reported to the ITU from the study
- SG 17 contacts for matters related to developing countries
  - Mohamed Elhaj (Sudan)
  - Patrick Mwesigwa (Uganda)
  - Raphael Nlend (Cameroon)

Business use of security standards

Q.1/17, Q.2/17

- Report with summary description of top security standards
  - Status and summary of standards • Who does the standard affect? • Business benefits • Technologies involved • Technical implications
- SG 17 is consulting with other standards development organizations to contribute to this effort
- Would benefit primarily to organizations planning to deploy ICT security systems
- SG 17 sees developing countries and countries with economies in transition to be especially interested in the results

Global cybersecurity information exchange framework (Cybersecurity information)

Q.4/17

- Structured information or knowledge concerning
  - The “state” of equipment, software or network based systems as related to cybersecurity, especially vulnerabilities
  - Forensics related to incidents or events
  - Heuristics and signatures gained from experienced events
  - Parties who implement cybersecurity information exchange capabilities within the scope of this framework
  - Specifications for the exchange of cybersecurity information, including modules, schemas, and assigned numbers
  - The identities and trust attributes of all of the above
  - Implementation requirements, guidelines and practices

Global cybersecurity information exchange framework (Purpose)

Q.4/17

- Enable global capabilities for the structured exchange of *cybersecurity information* by
  - identifying and incorporating existing “best of breed” platform standards
  - as necessary, making the existing standards more global and interoperable
- Move beyond guidelines and facilitate the scaling and broad implementation of core capabilities already developed within cybersecurity communities

Global cybersecurity information exchange framework (Strategic direction)

Q.4/17

- Profile of cybersecurity developments have scaled significantly with release of cybersecurity strategies and international initiatives – e.g., WTSA Res. 58, UK, US cybersecurity strategies
- National CIRTs are being created worldwide
- Realization that
  - global cooperation is essential to enhance cybersecurity
  - proven cybersecurity information exchange standards and enumerations already in use need to be "globalized"
  - "stovepiped" cybersecurity communities need to work together

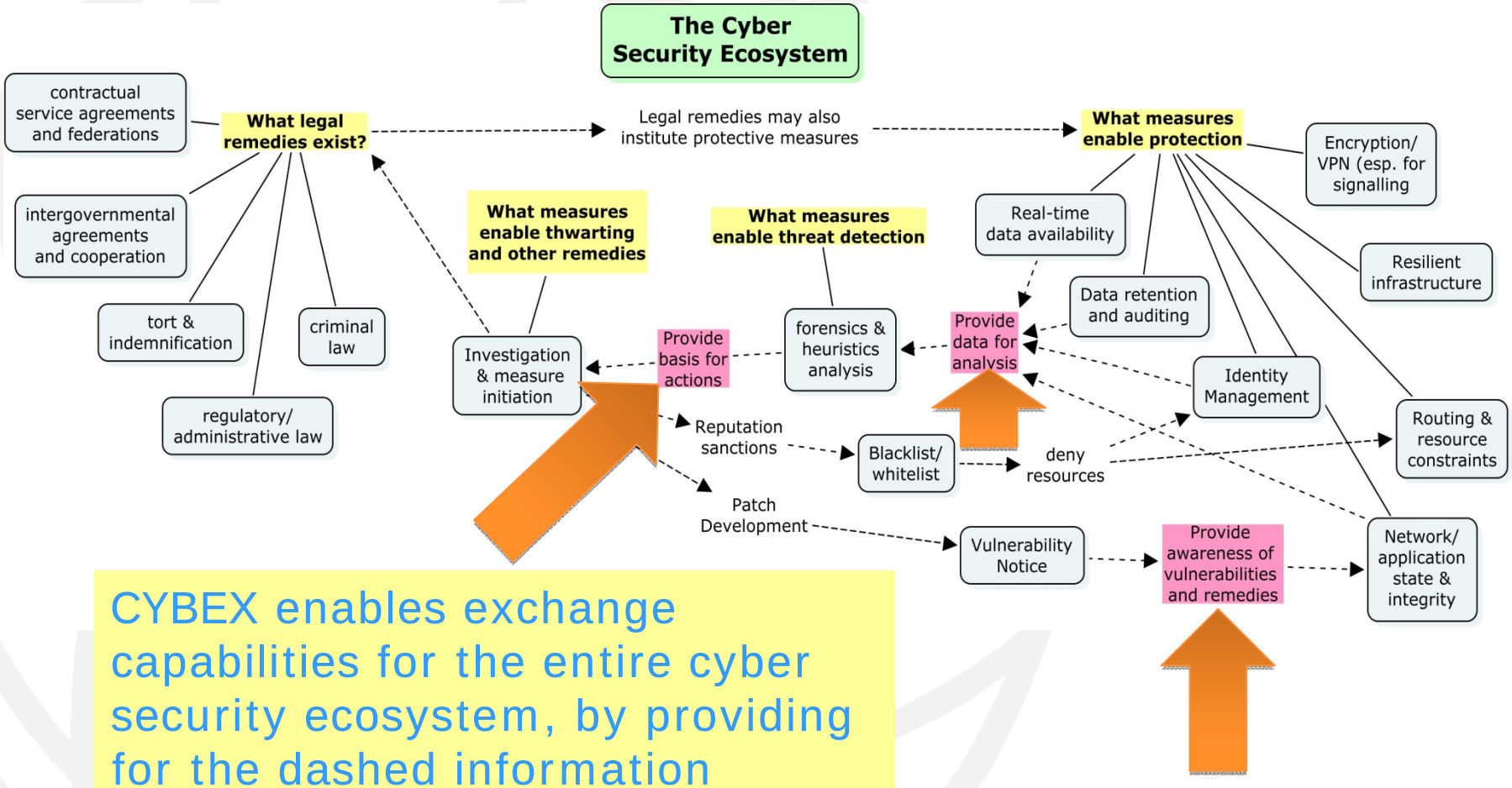
Global cybersecurity information exchange framework (Highlight of current activities)

Q.4/17

- Developing a framework Recommendation – X.cybex
  - A reponse to promote global, consistent, and interoperable processes for sharing incident-response related information
  - A large-scale effort to bring best of existing cybersecurity information exchange standards into the ITU and facilitating global interoperability and trust
    - for cybersecurity state, vulnerabilities, incidents, heuristics
  - Facilitated by
    - a global cybersecurity exchange identification scheme for cybersecurity organizations, information identifiers, and policies
    - use of extended validation certificates based on X.509
- Providing for close working relationship with principal CIRT/CERT organization (FIRST)
- Assisting developing countries to establish national CIRTS

Global cybersecurity information exchange framework (Capabilities and context)

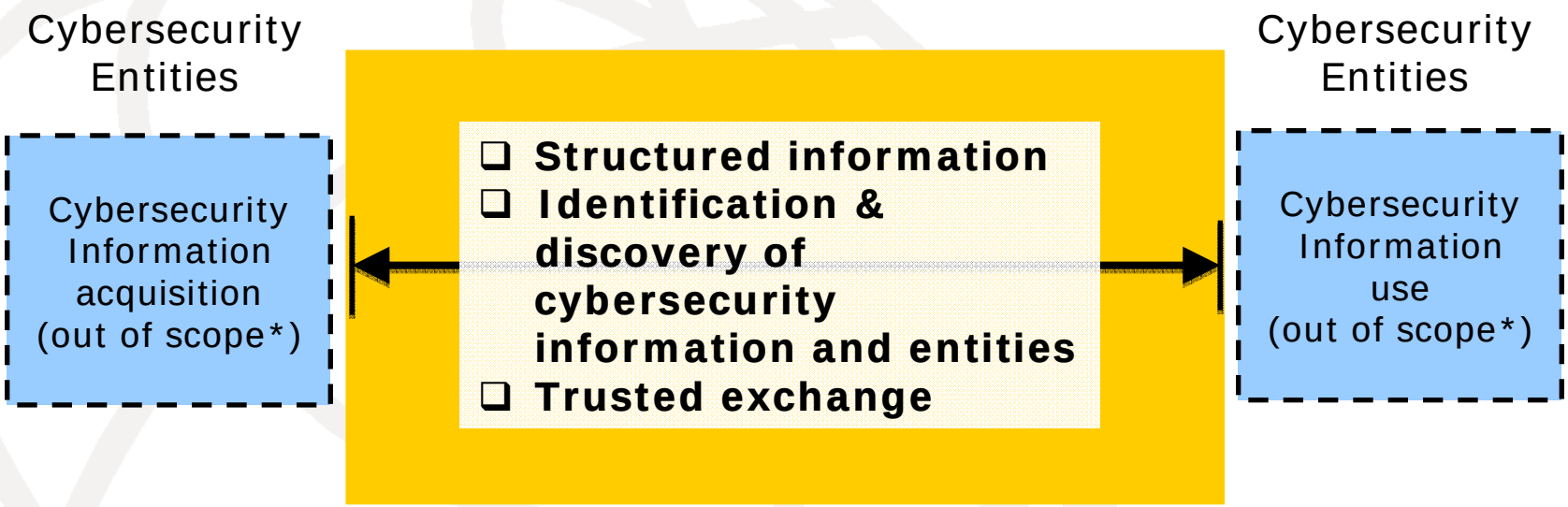
Q.4/17



CYBEX enables exchange capabilities for the entire cyber security ecosystem, by providing for the dashed information exchanges

Global cybersecurity information exchange framework

Q.4/17



*Some specialized cybersecurity exchange implementations may require application specific frameworks specifying acquisition and use capabilities

For each area: Identify existing standards and bring some of them into ITU-T as X-series Recommendations and supplement as needed for global interoperability

Cybersecurity – Work in progress

• **X.abnot**, Abnormal traffic detection and control guideline for telecommunication network • **X.bots**, Frameworks for botnet detection and response • **X.capec**, Common attack pattern enumeration and classification • **X.cce**, Common configuration enumeration • **X.cee**, Common event expression • **X.chirp**, Cybersecurity heuristics and information request protocol • **X.cpe**, Common platform enumeration • **X.crf**, Common result format • **X.cve**, Common vulnerabilities and exposures • **X.cvss**, Common vulnerability scoring system • **X.cwe**, Common weakness enumeration • **X.cwss**, Common weakness scoring system • **X.cybex**, Cybersecurity information exchange framework • **X.cybex.1**, An OID arc for cybersecurity information exchange • **X.cybex.2**, Use of XML namespace in the cybersecurity information exchange framework • **X.cybex-beep**, Definition of blocks extensible exchange protocol (BEEP) profile for cybersecurity information exchange framework • **X.cybex-disc**, Discovery mechanisms in the exchange of cybersecurity information • **X.cybex-tp**, Transport protocols supporting cybersecurity information exchange • **X.dexf**, Digital forensics exchange file format • **X.dpi**, Deep packet inspection exchange format • **X.eipwa**, Exchange of information for preventing web-based attacks • **X.gopw**, Guideline on preventing malicious code spreading in a data communication network • **X.gpn**, Mechanism and procedure for distributing policies for network security • **X.gridf**, SmartGrid incident exchange format • **X.iodef**, Incident object description exchange format • **X.oval**, Open vulnerability and assessment language • **X.pfoc**, Phishing, fraud, and other crimeware exchange format • **X.scap**, Security content automation protocol • **X.sips**, Framework for countering cyber attacks in session initiation protocol (SIP)-based services • **X.sisfreq**, Use cases and capabilities for cybersecurity information sharing and exchange • **X.tb-ucc**, Traceback use cases and capabilities • **X.teef**, Cyber attack tracing event exchange format • **X.trm**, Traceback mechanisms • **X.xccdf**, Extensible configuration checklist description format

Global cybersecurity information exchange framework (Challenges)

Q.4/17

- Keeping ahead of cybersecurity needs
  - vulnerabilities
  - incidents
- Getting isolated cybersecurity communities to cooperate effectively
  - includes use of a global cybersecurity exchange identification scheme
- Implementing needed identity management platforms and trust models in the infrastructure
  - widespread deployment of "Extended validation certificates" for organization/provider trust
  - that accommodate the diversity of parties and assurance levels/requirements
- Making cybersecurity “measurable”

Identity management (IdM) (overall objectives)

Q.10/17

- If implemented properly IdM is a security enabler by providing trust in the identity of both parties to an e-transaction
- Consequently, IdM is a very important capability for significantly improving security and trust
- IdM also provides network operators an opportunity to increase revenues by offering advanced identity-based services
- The focus of ITU-T's IdM work is on global trust and interoperability of diverse IdM capabilities in telecommunications. It is not in the development of standards for new IdM solutions. Rather it is focused on leveraging and bridging existing solutions

Identity management (IdM) (collaboration and coordination)

Q.10/17

- Effort started by IdM Focus Group which produced 6 substantial reports (265 pages) in 9 months
- JCA-IdM and IdM-GSI established by TSAG in December 2007 and renewed in April 2009
- Working collaboratively with other key bodies including: ITU-T SG 13 (Q.16/13), ISO/IEC JTC 1/SC 27, Liberty Alliance/Kantara Initiative, FIDIS, NIST, OECD, ENISA, OASIS, ...
- First ITU-T IdM Recommendation approved January 2009: **Y.2720** NGN identity management framework
- **X.Sup7**, Overview of identity management in the context of cybersecurity, approved February 2009
- **X.1250**, Capabilities for global identity management trust and interoperability, Approved September 2009
- **X.1251**, A framework for user control of digital identity, Approved September 2009

Identity management (IdM) (Recommendations in progress)

Q.10/17 and Q.16/13

- **X.1252,** Baseline identity management terms and definitions
- **X.1275,** Guidelines on protection of personally identifiable information in the application of RFID technology
- **Work in progress**

  • X.authi, Authentication integration in IdM • X.eaa, Entity authentication assurance • X.EVcert, Extended validation certificate framework • X.giim, Generic IdM interoperability mechanisms • X.idm-dm, Common identity data model • X.idm-ifa, Framework architecture for interoperable IdM systems • X.idmgen, Generic IdM framework • X.idmsg, Security guidelines for IdM systems • X.priva, Criteria for assessing the level of protection for personally identifiable information in IdM • Y.NGN IdM Mechanisms • Y.NGN IdM Requirements • Y.NGN IdM Use-cases (Supplement) • Y.NGN trusted SP (identity) requirements

Identity management (IdM) (Challenges for IdM)

Q.10/17

- Lack of identity federations based on standardized trust model and global interoperability of diverse identity management schemas are major inhibitors to wide scale deployment of IdM capabilities
- Terms and definitions alignment across standards development organizations
  - Work underway to develop an ITU-T Recommendation, X.idmdef on IdM terms and definitions

Security standardization strategy

Q.1/17

- Define a top-down approach to complement the contribution-driven work
  - to ensure the continued relevance of security standards by keeping them current with rapidly-developing technologies and operators' trends (in e-commerce, e-payments, e-banking, telemedicine, fraud-monitoring, fraud-management, fraud identification, digital identity infrastructure creation, billing systems, IPTV, Video-on-demand, grid network computing, ubiquitous networks, etc.)
  - to follow-up on considerable attention recently given to trust between network providers and communication infrastructure vendors, in particular for communication hardware and software security, issues of how trust can be established and/or enhanced would need to be considered

Conformance and interoperability testing (1)

Q.14/17

- **Demonstrate** how quality of Recommendations can be improved to facilitate:
  - product conformance
  - global interoperability
  - product qualification for the proposed ITU Mark
  - use of automated tools for more efficient product development and testing
- **Identify** relevant SG 17 Recommendations that would be needed for:
  - developing mandatory and optional conformance requirements based on X.290 methodology
  - developing Implementation Conformance Statement (ICS) proforma covering the static conformance requirements
  - formal languages that can be used to improve the quality of specifications
- Where possible, **develop test specifications**

Conformance and interoperability testing (2)

Q.14/17

- **Give confidence** in the use of ICT
- **Joint Coordination Activity on Conformance and Interoperability Testing (JCA-CIT)**
  - Established by SG 17, December 2006 (as JCA-Testing), renewed by TSAG in April 2009
  - Collaborate with Working Party 4/11, Test specifications (Andrey Koucheriavy, Russian Federation)
  - Collaborate with external organizations including ISO/CASCO, ETSI (TTCN-3, Z.160-series)

As a summary, we need

- to ensure the continued relevance of security standards as a mean for enhancing trust and confidence of users in networks, applications and services
- to address full cycle – vulnerabilities, threats and risk analysis; prevention; detection; response and mitigation; forensics; awareness
- to consider legal and regulatory aspects of cybersecurity, spam, identity/privacy
- for top-down strategic direction to complement bottom-up, contribution-driven process
- an effective cooperation and collaboration across the many bodies developing cybersecurity work
- to define a uniform language for security terms and definitions
- to identify the standards used in real-world applications among those many standards available in the field of telecommunications/ICT security
- to further work to determine how conformance and interoperability testing of implementations can be supported

Some useful web resources

- ITU Global Cybersecurity Agenda (GCA) http://www.itu.int/osg/csd/cybersecurity/gca/
- 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
- Lead Study Group 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
- ITU-T Recommendations http://www.itu.int/ITU-T/publications/recs.html
- ITU-T News http://www.itu.int/ITU-T/newslog/
- ITU-T Workshops http://www.itu.int/ITU-T/worksem/index.html

Arkadiy Kremer (Russia)
Chairman SG 17
February 2009

Hamadoun Touré
ITU Secretary-General
February 2009

Thank you for your attention