# ITU-T activities on security

## (focus on ITU-T Study Group 17)

17 September 2007

Georges Sebek
International Telecommunication Union (ITU)

Standards

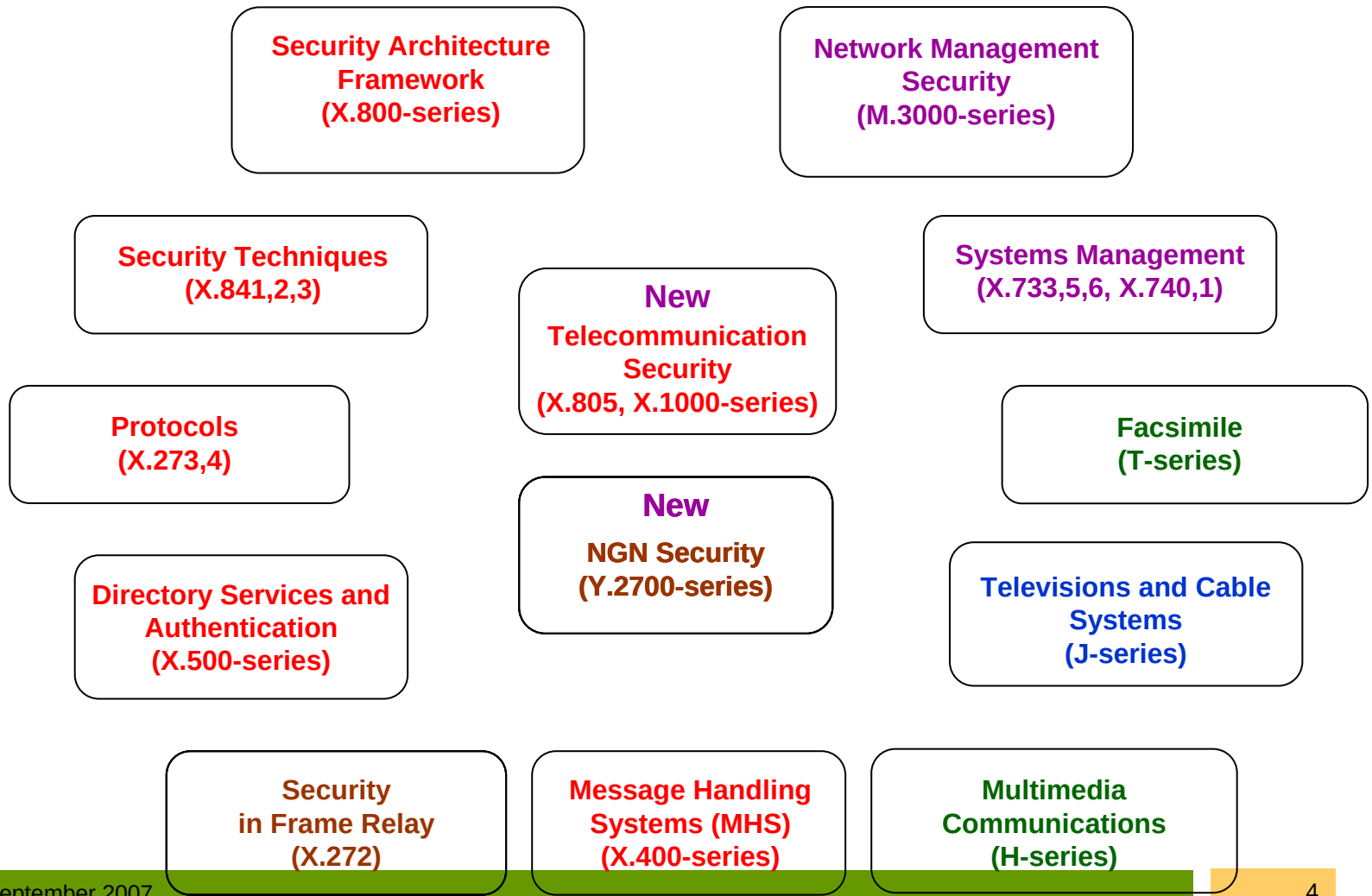
Cooperation

Awareness

# ITU-T Study Groups

- **SG 2 Operational aspects of service provision, networks and performance**
- SG 3 Tariff and accounting principles including related telecommunications economic and policy issues
- **SG 4 Telecommunication management**
- SG 5 Protection against electromagnetic environment effects
- SG 6 Outside plant and related indoor installations
- **SG 9 Integrated broadband cable networks and television and sound transmission**
- **SG 11 Signalling requirements and protocols**
- SG 12 Performance and quality of service
- **SG 13 Next generation networks**
- SG 15 Optical and other transport network infrastructures
- **SG 16 Multimedia terminals, systems and applications**
- **SG 17 Security, languages and telecommunication software**
- SG 19 Mobile telecommunication networks

# ITU-T Security Building Blocks



# Study Group 17: Security, languages and telecommunication software

- SG 17 is the Lead Study Group on telecommunication security - It is responsible for coordination of security across all study groups.
- Subdivided into three Working Parties (WPs)
  - *WP1 - Open systems technologies;*
  - *WP2 - Telecommunications security; and*
  - *WP3 - Languages and telecommunications software*
- Most (but not all) security Questions are in WP2
- Summaries of all draft Recommendations under development in SG 17 are available on the SG 17 web page at http://www.itu.int/itu-t/studygroups/com17

world summit on the information society
Geneva 2003 - Tunis 2005

BUILDING THE INFORMATION SOCIETY

International Telecommunication Union

**Telecom Systems Users**

**Telecom Systems**

## Telebiometrics
* Multimodal model framework
* System mechanism
* Protection procedure

**Q.8/17**

**Q.7/17**

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

## 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

**Q.4/17**

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

# Cybersecurity definition (draft Rec. X.1205)

Cybersecurity means the collection of tools, policies, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect organization and user's assets on the cyber environment. Organization and user's assets include connected computing devices, computing users, applications/services, communications systems, multimedia communication, and the totality of transmitted and/or stored information in the cyber environment.

Cybersecurity ensures the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The security properties include one or more of the following:

- Availability
- Integrity, which may include authenticity and non-repudiation
- Confidentiality

# Examples of recently approved security Recommendations (revision to well established standards, frameworks, technology or applications-related,…)

| | |
|---|---|
| M.3016.0, 1, 2, 3, 4 | Security for the management plane: Overview, Security requirements, Security services, Security mechanism, Profile proforma |
| X.509 | Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks |
| X.805 | Security Architecture for Systems Providing End-to-End Communications |
| X.893 | Information technology – Generic applications of ASN.1: Fast infoset security |
| X.1035 | Password-authenticated key exchange (PAK) protocol |
| X.1051 | Information security management system - Requirements for telecommunications (ISMS-T) |
| X.1081 | The telebiometric multimodal model - A framework for the specification of security and safety aspects of telebiometrics |
| X.1111 | Framework for security technologies for home network |
| X.1121 | Framework of security technologies for mobile end-to-end communications |
| X.1122 | Guideline for implementing secure mobile systems based on PKI |
| X.1141 | Security Assertion Markup Language (SAML 2.0) |
| X.1142 | eXtensible Access Control Markup Language (XACML 2.0) |
| X.1303 | Common Alerting Protocol (CAP 1.1) |
| Y.2701 | Security requirements for NGN release 1 |

# Extract from the current SG 17 security work

| Q. | Acronym | Title or Subject |
|---|---|---|
| 5 | X.akm | Framework for EAP-based authentication and key management |
| 6 | X.1205 | Overview of cybersecurity |
| 6 | X.idmf | Identity management framework |
| 6 | X.gopw | Guideline on preventing worm spreading in a data communication network |
| 7 | X.1051 (Revised) | Information security management guidelines for telecommunications based on ISO/IEC 27002 |
| 7 | X.rmg | Risk management guidelines for telecommunications |
| 8 | X.bip | BioAPI interworking protocol |
| 8 | X.tai | Telebiometrics authentication infrastructure |
| 9 | X.homesec-2, 3, 4 | Certificate profile for the device in the home network, User authentication mechanisms for home network service, Authorization framework for home network |
| 9 | X.msec-3 | General security value added service (policy) for mobile data communication |
| 9 | X.p2p-1 | Requirements of security for peer-to-peer and peer-to-multi peer communications |
| 9 | X.websec-3 | Security architecture for message security in mobile web services |
| 17 | X.csreq | Requirement on countering spam |
| 17 | X.fcsip | Framework of countering IP multimedia spam |

## Many more in SG 17 work plan … 45 x items

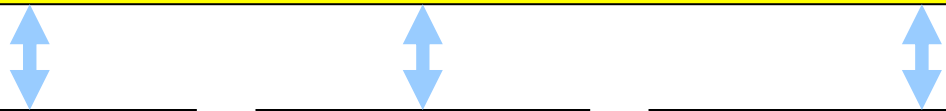
# Question 15/13, *NGN Security:* work in progress

| | |
|---|---|
| Y.IdMsec | NGN identity management security |
| Y.NGN AAA | AAA application for implementation of network and service security requirements over NGN |
| Y.NGN Authentication | NGN Authentication |
| Y.NGN Certificate Management | NGN certificate management |
| Y.SecMechanisms | NGN Security mechanisms and procedures |
| Y.SecReqR2 | Security requirements for NGN release 2 |

# Security standardization Collaboration is key factor 1/3

Specific Systems, Services, Applications Security in ITU-T are developed by SG 2, 3, 4, 5, 6, 9, 11, 13, 15, 16, 19

Core Technology and Common Security Techniques in ITU-T are developed by SG 17



ISO/IEC SC 27, 37 | IETF | ANSI, ETSI, OASIS, etc.

# Security standardization Collaboration is key factor 2/3

- World Standards Cooperation (WSC) **ISO, IEC, ITU**
- Global Standards Collaboration (GSC) **Regional, National SDOs and ITU-T, ITU-R**
  - exchange information between participating standards organizations to facilitate collaboration and to support the ITU as the preeminent global telecommunication and radiocommunication standards development organization
- **ISO IEC ITU-T** Strategic Advisory Group on Security (SAG-S)
  - To oversee standardization activities in ISO, IEC and ITU-T relevant to the field of security
  - To provide advice and guidance to the ISO Technical Management Board, the IEC Standardization Management Board and the ITU-T Telecommunication Standardization Advisory Group (TSAG) relative to the coordination of work relevant to security, and in particular to identify areas where new standardization initiatives may be warranted
  - To monitor implementation of the SAG-S Recommendations

# Security standardization Collaboration is key factor 3/3

- Security Standardization Exchange Network (SSEN)
  - an *informal* association of individual security practitioners with direct experience of, or strong interest in, security standardization
  - facilitate the informal exchange of information on security-standards-related matters to increase overall awareness of issues of common interest with the intention of helping to advance the development of needed standards and minimizing overlap and duplication of effort in security standards development
- SG 17 Security Standardization, Implementation and Evaluation Strategy Initiative
  - Why, What, How … to provide a security infrastructure
  - Strategy includes necessary collaboration within SG 17, ITU-T SGs, ITU, the telecom industry and SDOs.

# Focus Group: Security baseline for network operators (FG SBNO)

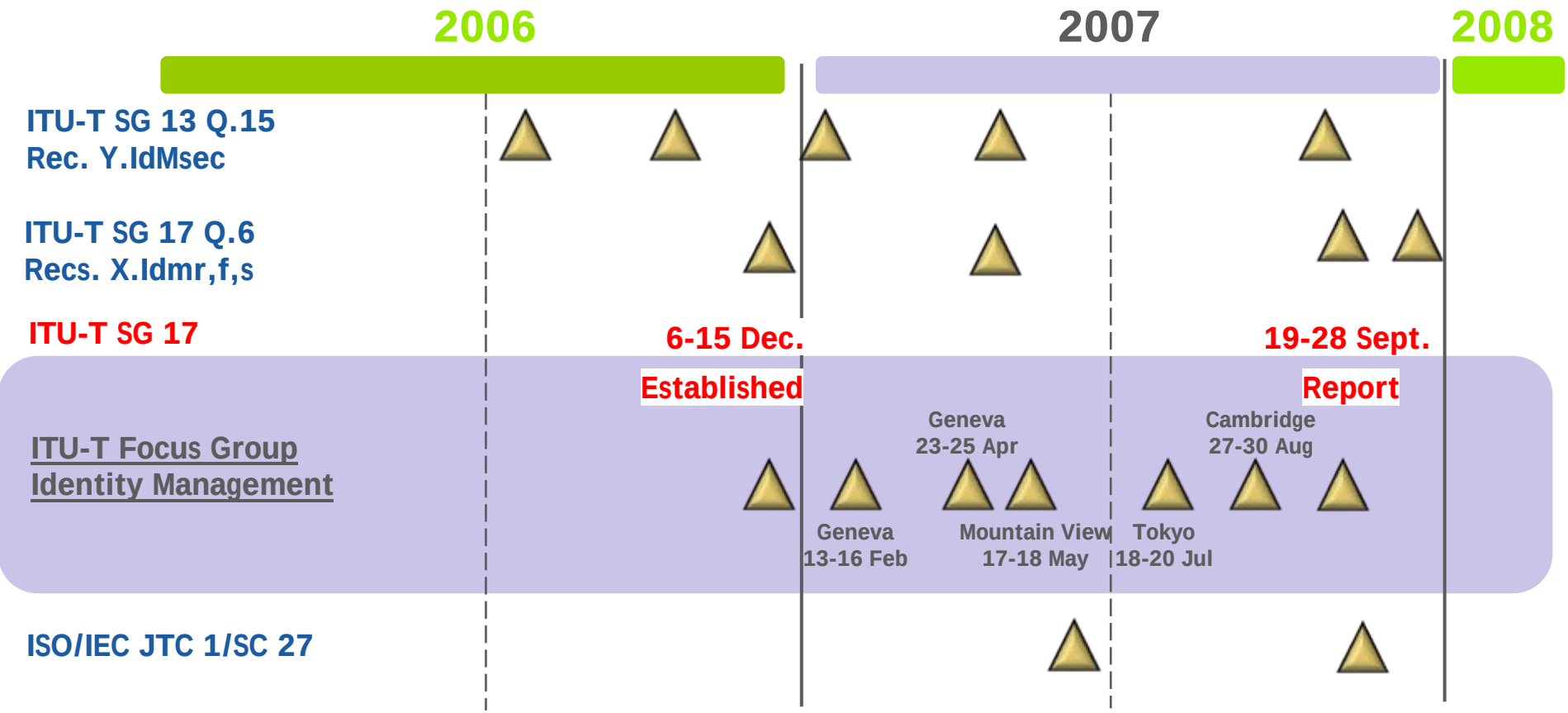
- Established October 2005 by SG 17
- Objectives:
  - Define a security baseline against which network operators can assess their network and information security posture in terms of what security standards are available, which of these standards should be used to meet particular requirements, when they 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.
- Achieved
  - Survey network operators by means of a questionnaire
- Next step:
  - Deliverable proposed to the September 2007 SG 17 meeting for progressing as an ITU-T publication

# Focus Group on Identity Management (FG IdM)

Established December 2006 by ITU-T SG 17

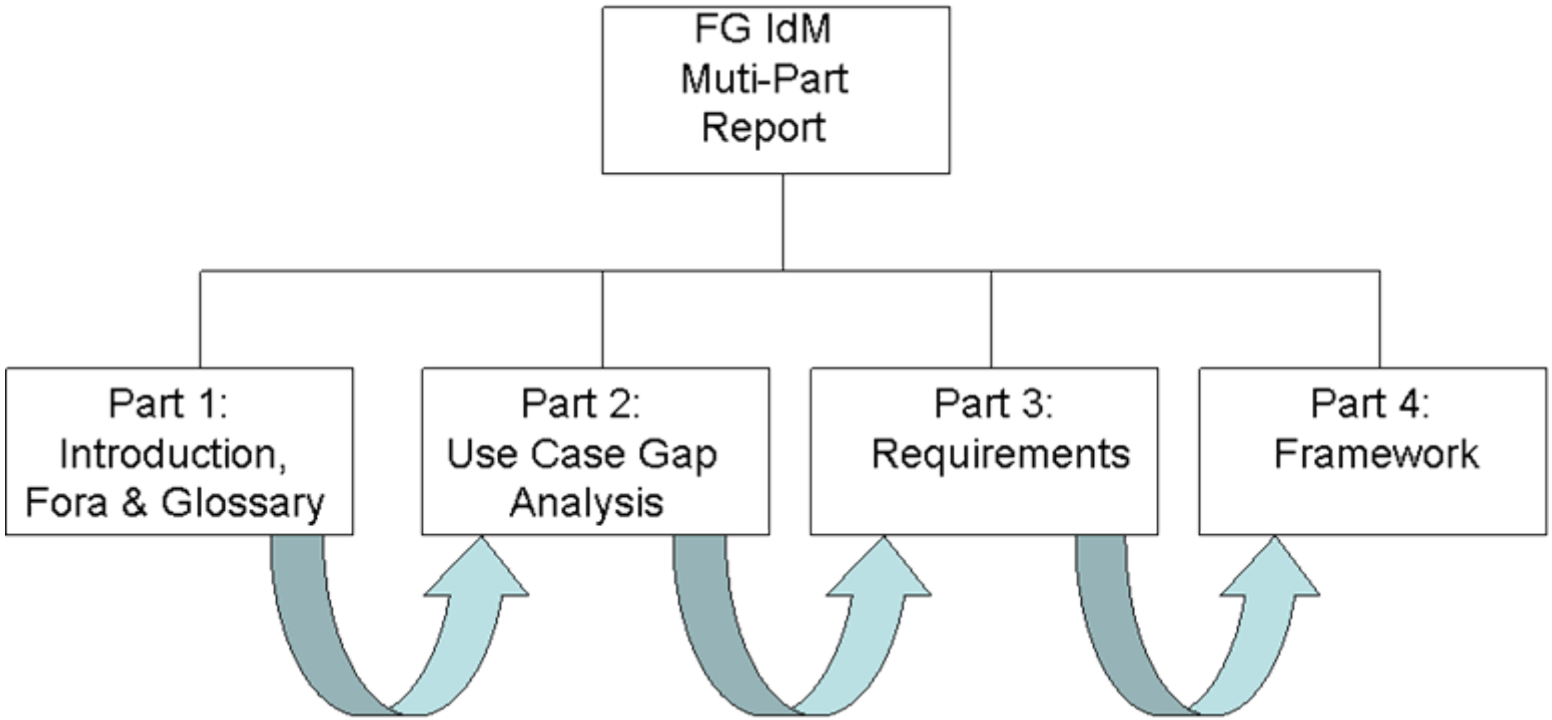
- Objectives of the FG IdM
  - perform requirements analysis based on uses case scenarios
  - identify generic IdM framework components
  - complete a standards gap analysis
  - identify new standards work and who should perform the work
- FG IdM met in February, April, May, July, August 2007
- Reports and deliverables for review at September 2007 SG 17 meeting and decision on the future of the Focus Group
- FG IdM structure
  - Ecosystem and Lexicon Working Group
  - Use Cases Working Group
  - Requirements Working Group
  - Framework Working Group

# FG IdM Timing



# FG IdM deliverables

http://www.itu.int/ITU-T/studygroups/com17/fgidm/index.html



# ICT security standards roadmap

- Part 1 contains information about organizations working on ICT security standards
- Part 2 is database of existing security standards
- Part 3 will be a list of standards in development
- Part 4 will identify future needs and proposed new standards
- Part 5 is now being built and includes Security Best Practices

ENISA and Network and Information Security Steering Group (NISSG) are now collaborating with ITU-T in the development of the Roadmap

# Roadmap access

- Part 2 currently includes ITU-T, ISO/IEC JTC 1, IETF, IEEE, ATIS, ETSI and OASIS security standards
- Since May 2007, the data is available in a database format to allow searching by organization and topic and to allow organizations to manage their own data
- Publicly available under *Special Projects and Issues* at:
  - http://www.itu.int/ITU-T/studygroups/com17/index.asp
- We invite you to use the Roadmap, provide feedback and help us develop it to meet your needs

# Other projects

- *Security in Telecommunications and Information Technology* – an overview of existing ITU-T Recommendations for secure telecommunications.

  http://www.itu.int/ITU-T/publications/index.html

- Security compendium:
  - catalogue of approved ITU-T Recommendations related to telecommunication security
  - extract of ITU-T approved security definitions
  - listing of ITU-T security related Questions

  http://www.itu.int/ITU-T/studygroups/com17/tel-security.html

# Observations

- Security is **everybody's business**
- Collaboration with other SDOs is **necessary**
- 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)

# Technical standards (ITU-T/ITU-D workshop, Hanoi, August 2007)

- Standards are essential
- Need to address wider needs (incl. from DC)
- Participation from the regions
  - To be increased
  - Tools exist
  - ITU, also other regional or international SDO
- Where to contribute
  - Several coming events are identified
- Multiplicity of actors, cost of meetings
  - Calendar of coming events
  - Online meetings

- Identified study items
  - 1 National reporting / information sharing ICT incidents
  - 2 Reporting format
  - 3 Interconnection
  - 4 Automatic detection / removal of malicious software
  - 5 Link to an ITU project
  - 6 Traceback
- Survey
  - In support of item 4: questionnaire to member states
- Impact of threats on NGN/IPv6
  - Workshop (mid-2008)

# 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
  e-mail: tsbsg17@itu.int
- Recommendations http://www.itu.int/ITU-T/publications/recs.html
- ITU-T Lighthouse http://www.itu.int/ITU-T/lighthouse
- ITU-T Workshops http://www.itu.int/ITU-T/worksem
- ICT Security Standards Roadmap
  http://www.itu.int/ITU-T/studygroups/com17/ict/index.html