CITEL's Focus on Cybersecurity and Critical Infrastructure Protection

Wayne Zeuch
CITEL
(Alcatel-Lucent)

ITU Regional Workshop on Frameworks for Cybersecurity and CIIP
Buenos Aires, Argentina
October 16-18, 2007

CITEL Inter-American Telecommunication Commission

ITU International Telecommunication Union

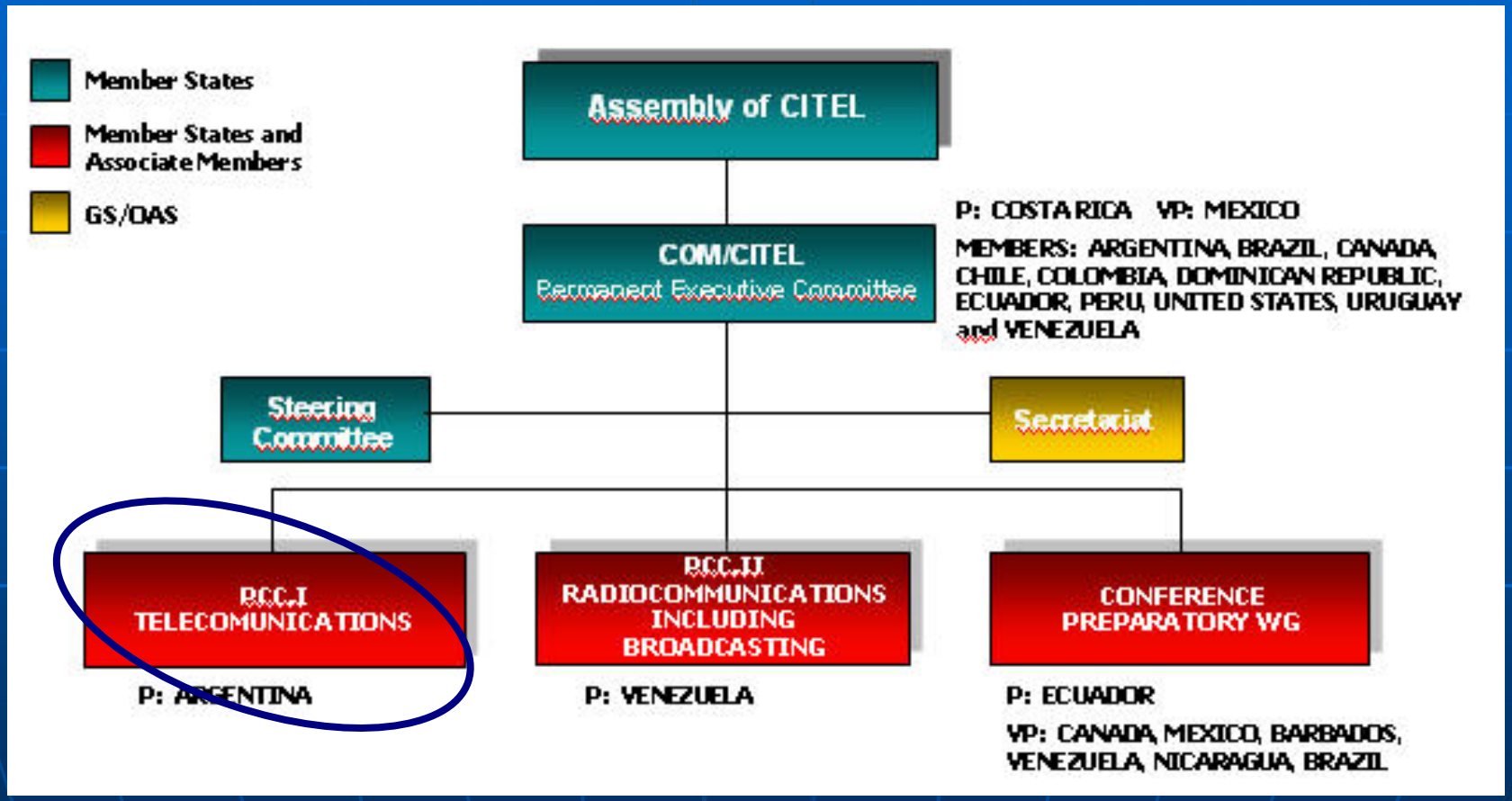
OAS Mandate*

Cybersecurity and Critical Infrastructure Protection

- CICTE, **CITEL**, and REMJA each represent a pillar of the Comprehensive Inter-American Cybersecurity Strategy
  - The multidisciplinary efforts of these bodies support the growth, development, and protection of the Internet and related information systems, and protect users of those information networks
  - The objective: Create and support a **culture of cybersecurity**
- Ongoing activities:
  - Coordination and **cooperation** among the Secretariats of CICTE, CITEL and the REMJA Group of Government Experts in Cyber crime
  - Strengthening coordination among the national authorities and entities, including the national CSIRTS, involved in addressing cybersecurity issues

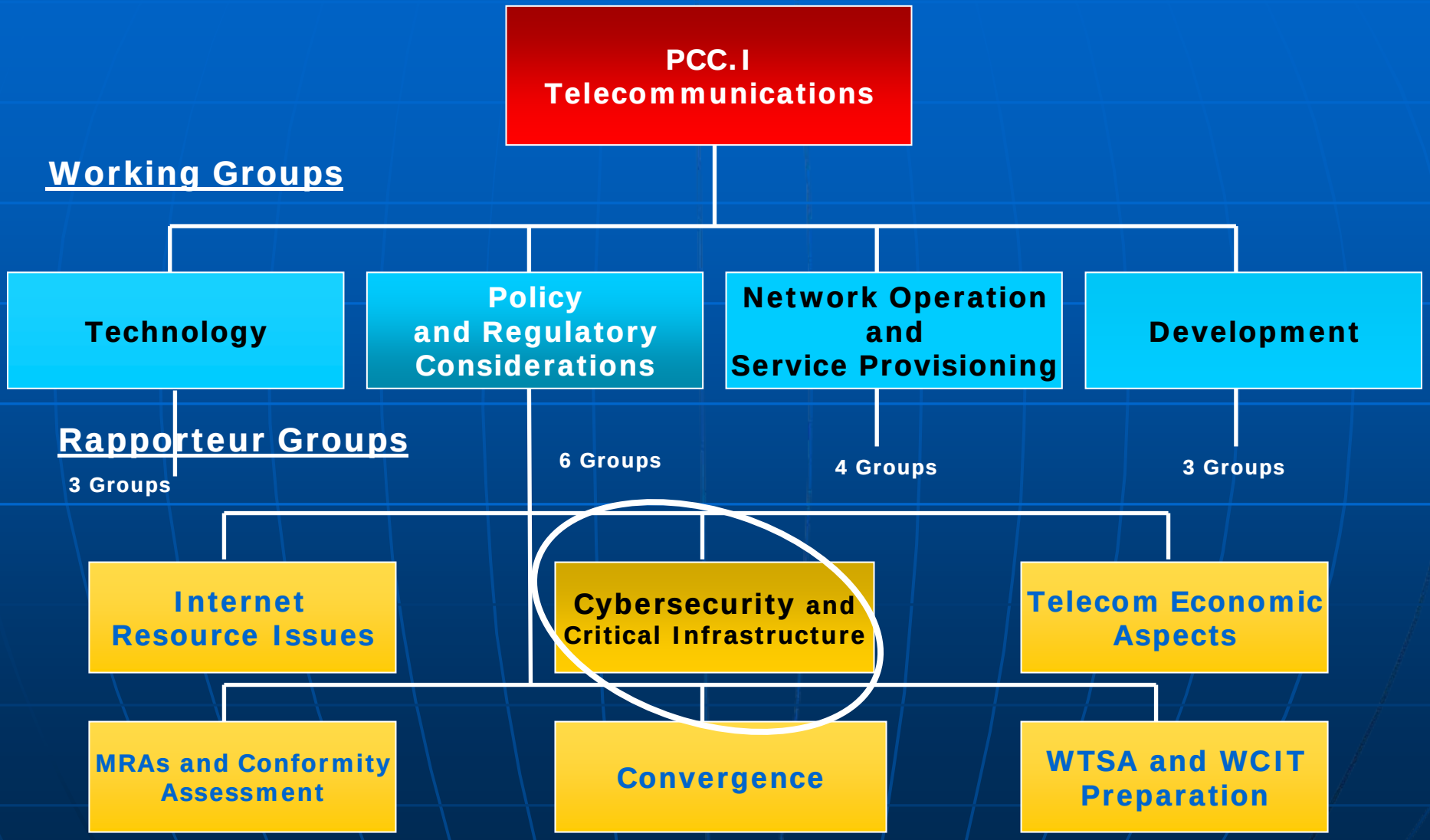
* "*Adoption of a Comprehensive Inter-American Strategy to Combat Threats to Cybersecurity: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity*", AG/RES. 2004 (XXXIV-O/04), (Adopted at the fourth plenary session held on June 8, 200 of XXXIV Meeting of the General Assembly of the OAS)

CITEL Organization



CITEL Inter-American Telecommunication Commission

CITEL-PCC.I Organization



CITEL PCC.I
Cybersecurity and Critical Infrastructure

Mandate:

- Study the security aspects related to communication network development
  - Role in supporting other critical infrastructures
  - Role of private sector in securing the communication network
  - Domestic and (Americas) Regional approaches required
- Assess current work in the OAS, ITU, and other fora on security issues and critical infrastructure
- Develop domestic and Regional approaches to network security, deployment strategies, information exchange, and outreach to the public and private sector
- Review frameworks and guidelines on networks and cybersecurity and their applicability within the Americas
- Foster dialog regarding the work of the ITU-T (SG 17) and other relevant fora

CITEL PCC.I
Cybersecurity and Critical Infrastructure

Terms of Reference:

- Develop domestic and Regional approaches to network security
  - Collect Regional “Best Practices”, taking into account ongoing activity in the ITU-D (Question 22/1)
  - Review various frameworks and guidelines for their applicability within the Americas Region
- Foster cooperation among OAS Member States
  - Help Administrations encourage network and service providers to implement technical standards for secure networks
  - Continue to coordinate the CITEL work on cybersecurity with the other OAS work of CICTE and REMJA

CITEL PCC.I
Cybersecurity and Critical Infrastructure

Terms of Reference (2):

- Identify and evaluate implementation and policy issues related to standards required for security of existing and future networks
  - Primary focus on ITU-T (SG 17)
  - Other SDOs and fora as appropriate (e.g., IETF, Regional SDOs)
- Identify (on a timely basis) obstacles to implementation of security measures in the networks of the Americas Region
- Establish liaisons with standards bodies and industry fora, as necessary, to advance work on OAS mandates

CITEL PCC.I

Technical Notebook

- Provides a formalized means of maintaining an archive of technical, best practices, policy, or regulatory information – made available to the OAS Member States and CITEL telecom industry members
- Documents relevant activities, completed or in progress
- As a ”living document”, it is updated on an ongoing basis with relevant information from contributions submitted to the Working Groups

Addressing Cybersecurity and CIP by archiving valuable information for the use of the telecom industry and in anticipation of future CITEL recommendations

CITEL PCC.I
"Cybersecurity" *Technical Notebook*

- Provides an archive of Cybersecurity information available to the telecommunications industry and the Member States
- Highlights ongoing Regional and International cybersecurity strategy activities
- Addresses aspects relevant to developing national cybersecurity strategies
- Addresses issues of spam, incident response, public-private partnerships, and the awareness-raising and application of relevant security standards
- Includes appendices with national experiences

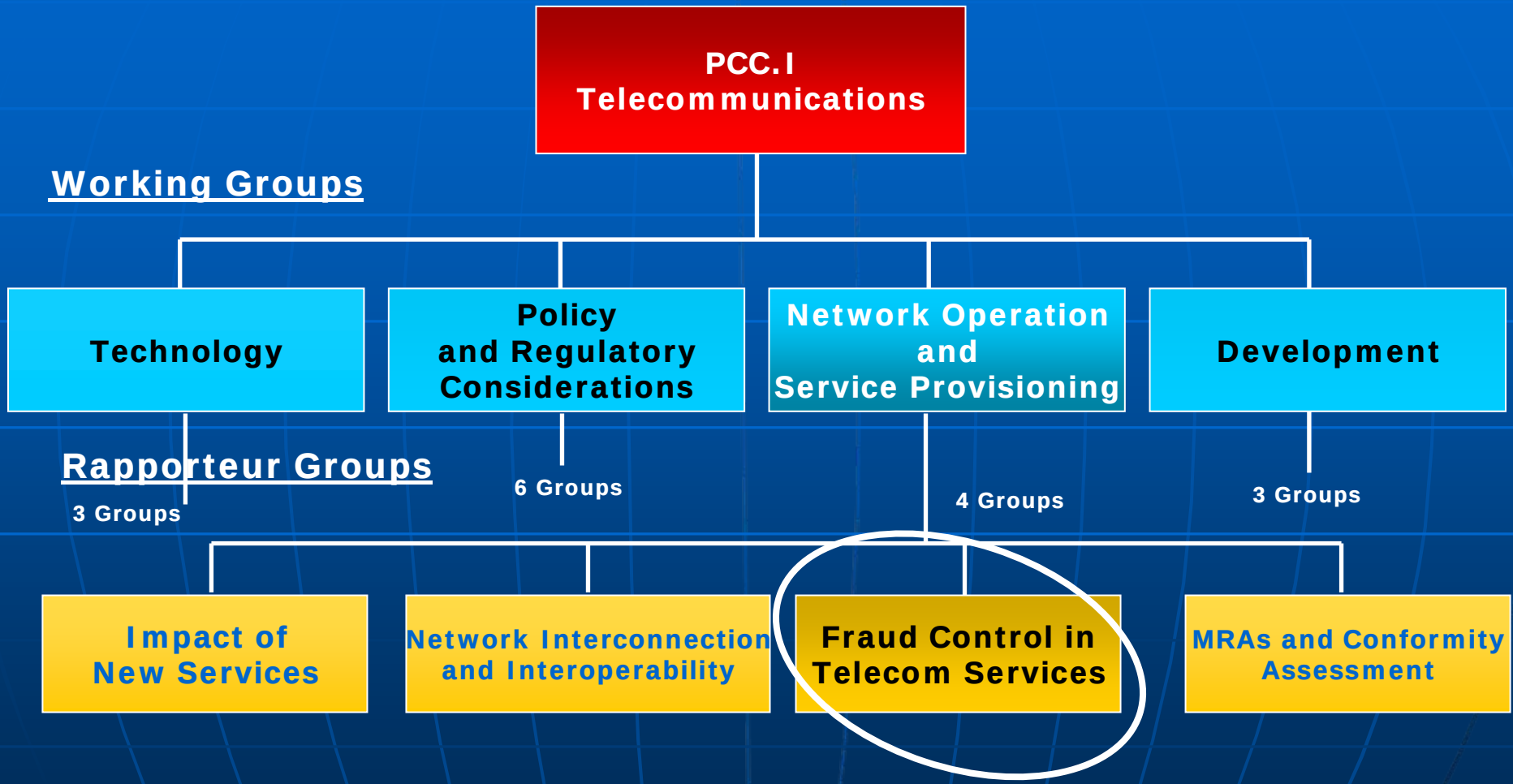
CITEL PCC.I

"Critical Infrastructure Protection" *Technical Notebook*

(proposed draft)

- To provide an archive of Critical Infrastructure Protection information available to the telecom industry and the Member States
- To highlight relevant CIP-related recommendations from the ITU and other relevant for a
- To discuss CIP needs, study constraints, and discuss strategies
- To document national CIP strategies of Member States
- To address new technical CIP issues as they arise

CITEL-PCC.I Organization



CITEL PCC.I
Fraud Control in Telecommunication Services

Mandate:

- Study and recommend strategies and Best Practices to detect and reduce fraud in telecommunications

Terms of Reference:

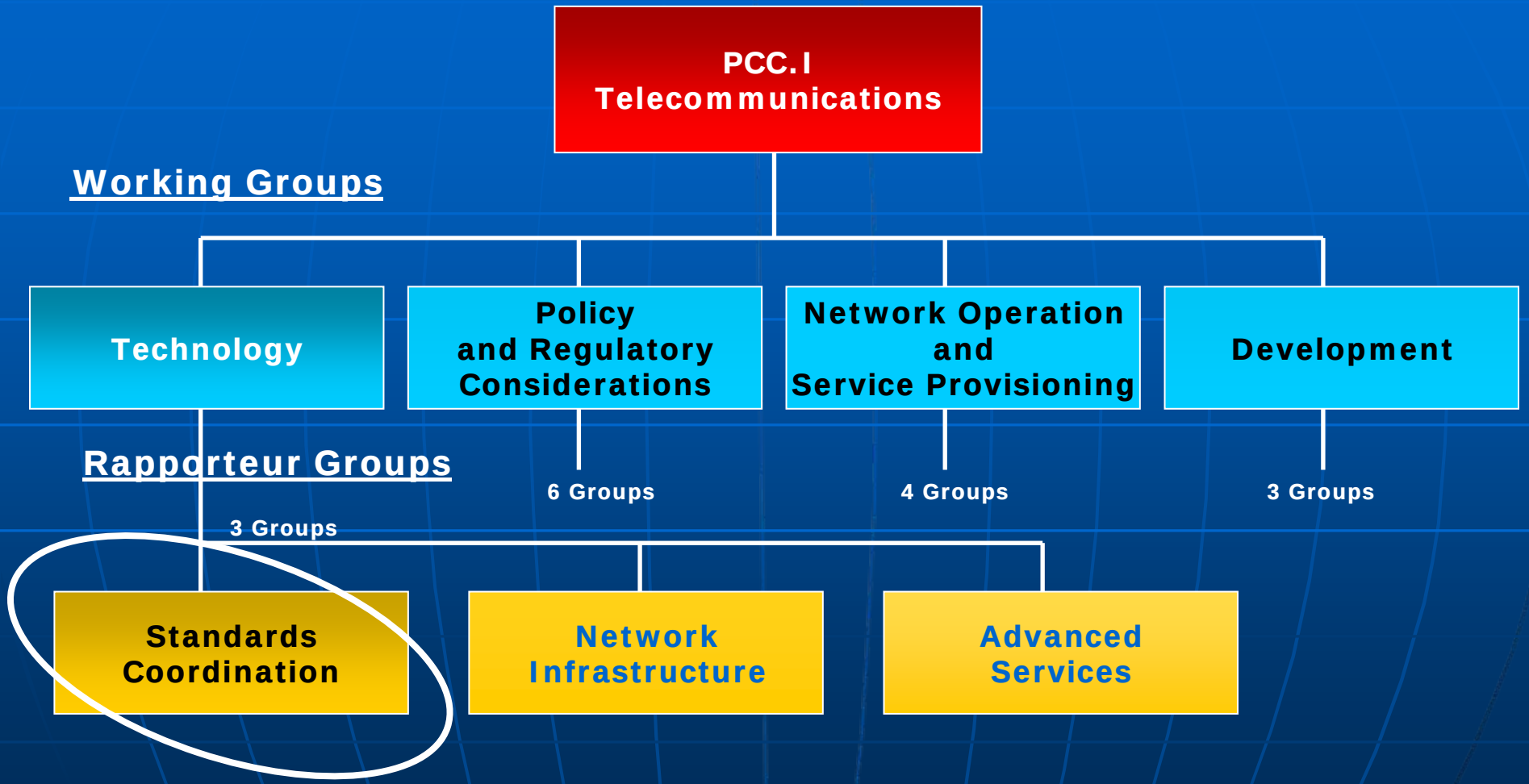
- Study different methods of perpetuating fraud and unauthorized access to networks
- Define strategies and Best Practices to increase network security and minimize the impact of fraud and unauthorized access
- Promote dialog and Regional exchange of information on fraud in telecommunications

CITEL PCC.I

"Fraud in the Provision of Telecom Services *Technical Notebook* (proposed draft)

- To provide an archive of fraud-related information contributed to CITEL PCC.I and available to the telecom industry and the Member States
- To include fraud classification, technological tools to minimize the impact of fraud, and regulatory/judicial/administrative tools to tackle fraud
- To include results and analysis of questionnaires on fraud sent to the Region
- To track the activities of bodies conducting fraud research
- To include fraud cases experienced by CITEL members and assess the impacts of fraud
- To archive presentations, summaries, and conclusions of CITEL workshops on fraud-related issues
- To archive Recommendations on fraud approved for the Region

CITEL-PCC.I Organization



CITEL PCC.I
Standards Coordination

Mandate:

- Focus on the study of standards that are necessary for the smooth transition to Next Generation Networks (NGN).
- Address issues relating to the convergence of existing networks in a way that maintains interoperability across the Region.
- Make specific recommendations (Coordinated Standards Documents, Technical Notebooks, etc.) that best serve the current and future needs of the users of these networks throughout the Region.

CITEL PCC.I
Standards Coordination

Terms of Reference:

- Identify and evaluate technical issues related to the **service, architecture** and **protocol standards** required for the interconnectivity and interoperability of existing and future communications networks (wireline and wireless) across the Region.
- Draw primarily on the work of **existing standards-setting bodies**, including the ITU-T, IETF, and other fora as appropriate.
- Develop **Technical Notebooks** that best serve the current and future needs of the users of telecommunications networks throughout the Region.
- Establish **liaisons** with other standards bodies and industry fora as necessary to progress the work.

CITEL PCC.I
Standards Coordination

Standards topics identified:

- **Communications system security (security framework, protocols, lawful intercept, privacy, fraud prevention, cyber crime)**
- Multimedia service definition and architectures
- Signaling requirements and protocols (converged networks)
- IP-based services (Voice over IP, Video over IP, etc.)
- Emergency services;
- Interworking between traditional telecommunication networks and evolving networks
- Metropolitan and Long haul optical transport networks
- Metropolitan and Long haul optical transport networks
- Access network transport (LANs, Wireless LANs, xDSL, Ethernet, cable modem, fiber, etc.)
- Terminals (PC, TV, PDA, phone, codecs, etc.)
- Management of communications services, networks and equipment
- Network aspects of IMT-2000 and beyond (wireless internet, harmonization and convergence, network control, mobility, roaming, etc.)
- Numbering, Naming and Addressing (ENUM)
- Performance and QoS

CITEL PCC.I
Coordinated Standards Document

- A documented case for the endorsement of a standard. Each CSD includes:
  - a summary of the standard development and approval (in the ITU-T, IETF, or other relevant forum)
  - a summary of the standard
  - a summary of presentations and discussions of the standard within PCC.I
  - a discussion of the relevance of the standard to the Americas Region
  - a recommendation that CITEL-PCC.I endorse the standard
  - a recommendation for future work on the standard's topic (if any)

CITEL-PCC.I Resolutions Endorsing Standards for the Americas Region

Standard	Date
Gateway Control Protocol	March 2001
Intelligent Networks Capability Set 3	March 2001
Intelligent Networks Capability Set 4	Dec 2002
ITU-T Y.2000-Series Recs for NGN (SG13)	Sept 2003
ANSI-41 Evolved Core Network with CDMA2000 Access Network	Sept 2003
GSM Evolved UMTS Core Network with UTRAN Access Network	Sept 2003
Security Architecture for the Internet Protocol (IPsec)	**March 2004**
Security Architecture for Systems Providing End-to-End Communications (ITU-T Rec. X.805)	**March 2004**

Standard	Date
Packet-Based Multimedia Communications Systems (ITU-T Rec. H.323)	March 2004
Interworking Between SIP and BICC Protocols or ISUP (Rec. Q.1912.5)	Sept 2004
SIP: Session Initiation Protocol	April 2005
ITU-T Rec. G.993.2 , VDSL2: Very High Speed DSL-2 Transceivers	Sept 2006
ITU-T Rec. J.122, "Second-Generation Transmission Systems for Interactive Cable Television Services – IP Cable Modems"	Sept 2006
Internet Protocol Version 6 (IPv6)	Sept 2006
E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)	Sept 2007

CITEL PCC.I

"Next Generation Networks: Standards Overview"

Technical Notebook

- Provides an archive of NGN technical information (including security-related topics) that is available to the telecom industry and the Member States
- Identifies NGN related standards that the Standards Coordination Group is studying, including relevant security standards such as:
  - ITU-T Security Architecture (Rec. X.805)
  - Internet Protocol Security (IPsec)
  - Internet Key Exchange (IKE)
  - Encryption Key Management
- Documents NGN standards, completed or in progress, which may be considered for future development into a CSD in accordance with the approval procedures of the Technology WG

Addressing Cybersecurity and CIP by archiving standards summaries in anticipation of future endorsement

PCC.I Workshops

Workshop	Location	Date
Cybersecurity	Quito, Ecuador	March 2004
Fraud: Impact on Provision of Telecom Services for Users, Operators , and States	videoconference	June 2007
Fraud: Impact on Provision of Telecom Services in the Americas	Mendoza, Argentina	Sept 2007

Addressing Cybersecurity and CIP by socializing key issues and best practices via workshops and seminars

Summary

- CITEL continues to address Cybersecurity and Critical Infrastructure Protection and has initiated new work in several key areas
- CITEL is coordinating with its Regional OAS partners (CICTE, REMJA) and is partnering with the ITU and other international bodies to utilize the widest available experience and best practices to address security issues for the Americas Region
- CITEL is not only collecting experiences and data on Cybersecurity and CIP from its members, but is also actively engaged in discussions of national strategies and best practices, leading to recommendations for the Americas Region

Summary (2)

- CITEL is utilizing workshops and Technical Notebooks to increase awareness of cybersecurity and CIP issues and to assess best practices and strategies in order to increase security and mitigate the effects of cyber crime and fraud
- CITEL is utilizing Coordinated Standards Documents to increase awareness of relevant security standards and to endorse the use of those standards in the Region
- Continued cooperation within the Americas Region and continued input from its members on cybersecurity experiences and strategies will allow CITEL to remain focused on the most relevant security issues so as to provide recommendations for the Region and provide value to other bodies internationally

Thank You!

MUCHAS GRACIAS

Wayne Zeuch
Rapporteur, CITEL PCC.I Standards Coordination

Alcatel-Lucent
zeuch@alcatel-lucent.com