# ITU Mandate and Activities Related to Cybersecurity

***Subregional Seminar on Cybersecurity for Information and Communication Networks***

**21 June 2005 Lima, Peru**

**Christine Sund**
**Policy Analyst**
**ITU Strategy and Policy Unit**
**< christine.sund @ itu.int >**

International Telecommunications Unit

# Agenda

- **Brief overview of ITU activities**
- **A global approach: ITU initiatives related to cybersecurity**
- **ITU mandate and cybersecurity**
- **Cybersecurity and the World Summit on the Information Society (WSIS)**
- **Local activities: ITU-D cybersecurity initiatives**
- **Way forward: WSIS Thematic Meeting on Cybersecurity and other initiatives**
- **Conclusion**

International Telecommunications Unit

# Overview of ITU Activities

International Telecommunications Unit

# International Telecommunication Union

- Impartial international organization that allows governments and businesses to work together:
  - to coordinate operation of telecom networks and services
  - to globally advance the development of telecommunications technology
- Founded in 1865, it is the oldest specialized agency of the UN system (140 years in May 2005)
- Unique partnership of governments and industry: **189 Member States, 620 Sector Members** and **100 Associates** (May 2005)

International Telecommunications Unit

# ITU structure

**Radiocommunication Sector (ITU-R)**

- Management of the radio frequency spectrum and satellite orbits globally

**Telecommunication Standardization Sector (ITU-T)**

- Establishing internationally agreed technical and operating standards for networks and services

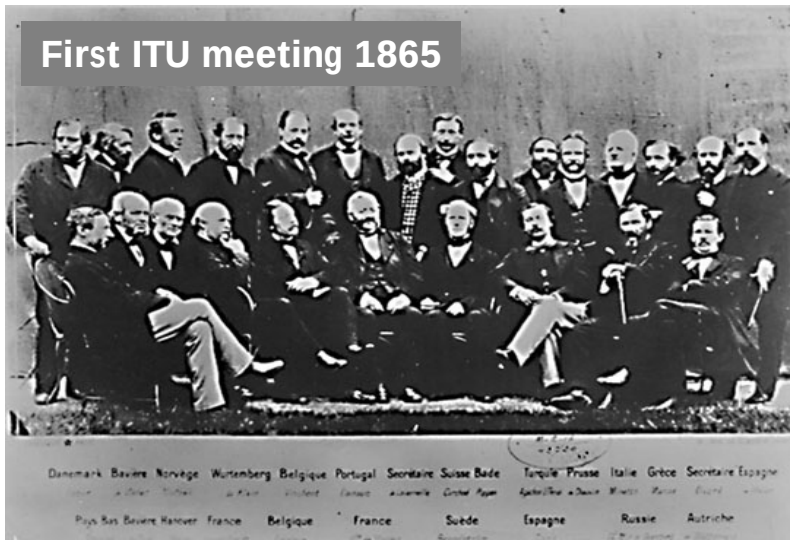
**Telecommunication Development Sector (ITU-D)**

- Promoting access in developing countries to information and communication technologies (ICTs)

International Telecommunications Unit

# ITU mandate:conferences and meetings

- ITU Plenipotentiary Conferences and Council Meetings
- World Radiocommunication Conferences (WRC)
- World Telecommunication Standardization Assembly (WTSA)
- Telecommunication Standardization Advisory Group (TSAG)
- Telecommunication Development Advisory Group (TDAG)
- ITU Global Symposium for Regulators (GSR)



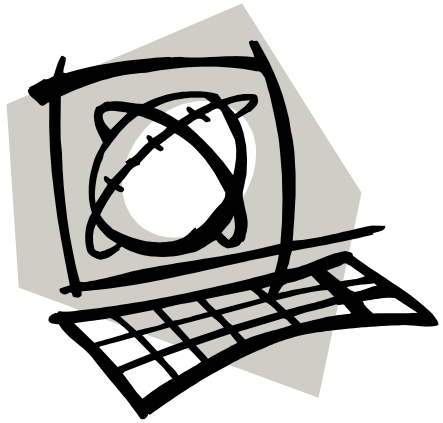

International Telecommunications Unit

# ITU Security-Related Activities

International Telecommunications Unit

# Role of critical network infrastructures

- In the 21st century, most critical infrastructures are dependent on information and communications systems that span the globe



- Dependencies vary from nation to nation; however, nearly all nations already depend on critical network infrastructures or will in the future.

International Telecommunications Unit

# Some ITU security related activities

- One of the most important security standards used today is X.509, an ITU recommendation for electronic authentication over public networks. X.509 is the definitive reference for designing secure applications for the Public Key Infrastructure (PKI) and is widely used for securing the connection between a user's web browser and the servers providing information content or e-commerce services.

- Ongoing work in security management, telebiometrics, mobile security
  www.itu.int/itut/studygroups/com17/cssecurity.html

International Telecommunications Unit

# ITU security related activities (cont'd)

- ITU Manual on Security in Telecommunications and Information Technology
  http://www.itu.int/ITU-T/edh/files/security-manual.pdf

- Over 70 ITU recommendations/standards focusing on security have been published. These include security from network attacks, theft or denial of service, security for emergency telecommunication, etc.

- Several ITU workshops and meetings on protecting critical network infrastructures, spam and cybersecurity have been conducted.

International Telecommunications Unit

# ITU Mandate & Cybersecurity

International Telecommunications Unit

# ITU mandate and cybersecurity

- **UN Resolution 57/239 (2002):** *"Creation of a global culture of cybersecurity"*
- **UN Resolution 58/199 (2004):** *"Creation of a global culture of cybersecurity and the protection of critical information infrastructure"*
- **ITU Plentipotentiary Resolution 130 (2002):** *"Strengthening the role of ITU in information and communication network security"*
- **WTDC (2002):** Cybersecurity is one of the six priority domains in WTDC2002 IsAP Programme 3:
  http://www.itu.int/ITU-D/e-strategy/WSIS/C5.html

International Telecommunications Unit

# ITU WTSA - October 2004

- **Resolution 50** *on Cybersecurity*
- **Resolution 51** *on Combating spam*
- **Resolution 52** *on Countering spam by technical means*

As interest groups are starting to recognize the importance of improved international cooperation in the field of spam and cybersecurity, the role of the ITU in contributing to further development in the area through improving the exchange of best practices between developed and developing countries, creating harmonized legal frameworks and cooperating with other international organizations working in the area, has also been recognized.

International Telecommunications Unit

# ITU, World Summit on the Information Society (WSIS) & Cybersecurity

International Telecommunications Unit

# World Summit on the Information Society

In 2001, the ITU Council decided to hold the World Summit on the Information Society (WSIS) and in Resolution 56/183, the United Nations' General Assembly endorsed the framework for the Summit adopted by the ITU Council:

*inviting* ITU to assume the leading managerial role in the executive secretariat of the Summit and its preparatory process, a well as;

*inviting* the *g*overnments to participate actively in the preparatory process of the Summit and to be represented in the Summit at the highest possible level.

International Telecommunications Unit

# World Summit on the Information Society

- First phase of the Summit held in Geneva in December 2003, the second phase to be held in **Tunis in November 2005**.
- The WSIS Declaration of Principles states that strengthening the trust framework, including information security and network security, authentication, privacy and consumer protection, is a prerequisite for the development of the Information Society and for **building confidence** among users of ICTs.
- **A global culture of cybersecurity** needs to be actively promoted, developed and implemented in cooperation with all stakeholders and international expert bodies.

International Telecommunications Unit

# World Summit on the Information Society

- **WSIS Declaration of Principles**

  Build confidence and security in the use of ICTs (Section 5, page 5, paragraphs 35, 36, 37)
  - Strengthening the trust framework
  - Promoting a global culture of cybersecurity
  - Preventing cybercrime/misuse of ICTs
  - Fighting spam (unsolicited electronic messages)

- **WSIS Plan of Action**

  Need to take appropriate action at national and international levels (WSIS Plan of Action, paragraph C5 and its subgroups)

International Telecommunications Unit

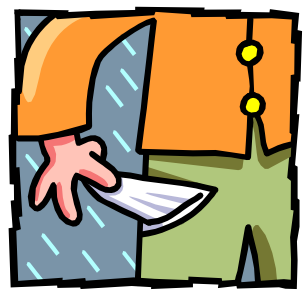
# Developing/Transitional Countries & Cybersecurity

International Telecommunications Unit

# Cyberspace makes all countries border each other

- International cooperation, on both technical (standardization) and policy (legislation and enforcement) sides, has been recognized as a key element to solving the problem.

- Developing countries are also forced to deal with the problem of spam, which has even more dramatic consequences on Internet access than in developed economies. Developing countries often lack the technical, knowledge and financial resources to face it.



International Telecommunications Unit

# Views of developing countries

Joint contribution from Kenya, Sudan, Tanzania and Zambia at ITU meeting on countering spam:

- "In some countries, the **consumers begin to shun the Internet** or just reduce their use of the Internet."
- "It also causes a Denial of Service on our networks as well as a **danger to development** in the sector."
- "Spam is a **global problem** that should be resolved in collaboration with all other nations."

International Telecommunications Unit

# ITU-D and Activities Related to Cybersecurity

International Telecommunications Unit

# ITU-D and cybersecurity - *Background*

- ITU-D activities in cybersecurity started at the launch of the ITU Electronic Commerce for Developing Countries in March 1998.
- Priority was given to assisting developing countries to implement secure and high trust e-commerce platforms.
- Projects delivering cybersecurity solutions for e-commerce transactions implemented in Brazil, Burkina Faso, Cambodia, Morocco, Peru, South Africa, Senegal, Turkey, Venezuela and Vietnam.
- Participation of industry security companies in e-commerce security and trust deployment.
- Cybersecurity and E-legislation were included as two of the six priority domains of the new programme adopted at the World Telecommunication Development Conference (WTDC) in Istanbul 2002.

International Telecommunications Unit

# ITU-D E-Strategies Unit

- **Goal:** Use ICTs to reduce the social divide, improve the quality of life and facilitate entry into the information society for developing countries.
- **Method:** Leveraging the potentials of the Internet as a low-cost channel for the delivery of online services in Health (**e-health**), Business (**e-business**), Education (**e-education**) and Government Services (**e-government**).

➔ **Challenge:** To move from simple online dissemination systems to the conduct of critical transactions in e-health, e-business and e-government **requires security and confidence** in the networks, applications and services.

International Telecommunications Unit

# Mandate for security, confidence and trust

| WSIS Plan of Action, Dec 2003 | Reference to ITU WTDC (Istanbul Action Plan -Programme 3), March 2002 |
|---|---|
| **C5) Building confidence and security in the use of ICTs**<br><br>12. Confidence and security are among the main pillars of the information society.<br>a) Promote cooperation among governments at the UN and with all stakeholders enhance user confidence, build trust, and protect both data and network integrity; consider existing and potential threats to ICTs; and other information security and networks security issues. | Two out of the six priority areas of Istanbul Action Plan Programme 3 address Security, confidence and E-legislation. ITU-D has, through this, been mandated to enhance security and build confidence in the use of public networks for e-services/applications. |
| b) Governments in cooperation with the private sector, should prevent, detect and respond to cybercrime and misuse of ICTs.<br>c) Governments, and other stakeholders should actively promote user education and awareness about online privacy and the means of protecting privacy.<br>d) Take appropriate action on spam at national and international levels.<br>e) Encourage the domestic assessment of national laws with a view to overcoming any obstacles to the effective use of electronic documents and transactions including electronic means of authentication. | Through IsAP3 provide assistance to Member States in developing laws and model legislation for e-services/ applications, prevention of cyber crime, security, ethical issues and data privacy. |

# Mandate for security, confidence and trust

| WSIS Plan of Action, Dec 2003 | Reference to ITU WTDC (Istanbul Action Plan -Programme 3), March 2002 |
|---|---|
| f) Further strengthen the trust and security framework with complementary and mutually reinforcing initiatives in the fields of security in the use of ICTs… | Through IsAP3 identify security requirements and propose solutions for the development of secure IP infrastructure for e-services/ applications on various types of networks using relevant technologies. |
| g) Share good practices in the field of information security and network security and encourage their use by all parties concerned.<br><br>h) Invite interested countries to set up focal points for real-time incident handling and response, and develop a cooperative network between these focal points for sharing information and technologies on incident response. | Develop tools to facilitate the exchange of best practices on IT security, legal issues related to the areas of activity of the IsAP3 Programme. |
| i) Encourage further development of secure and reliable applications to facilitate online transactions.<br><br>j) Encourage interested parties to contribute actively to the ongoing UN activities to build confidence and security in the use of ICTs. | It is necessary to address the security concerns in order to leverage the potentials of public networks as vehicles for delivering affordable value-added e-services/ applications. |

# ITU-D's mandate for security - *Activities*

| WSIS Plan of Action, Dec 2003 | Reference to ITU WTDC, March 2002 (Istanbul - Programme 3) |
|---|---|
| **C5) Building confidence and security in the use of ICTs**<br>12. Confidence and security are among the main pillars of the information society.<br>a) Promote cooperation among the governments at the UN and with all stakeholders at other appropriate for a to enhance user confidence, build trust, and protect both data and network integrity; consider existing and potential threats to ICTs; and other information security and networks security issues. | Two out of the six priority areas of Istanbul Action Plan Programme 3 address Security, confidence and E-legislation. ITU-D has, through this, been mandated to enhance security and build confidence in the use of public networks for e-services/applications. |

**I ) ITU-D activities in security and confidence building**

*Implementing projects on security and trust for e-applications*

Projects using advanced security and trust technologies based on Public Key Infrastructure (PKI) including biometric authentication, smart cards, ITU-T X.509 digital certificates and digital signature techniques have been deployed and operational in Bulgaria, Burkina Faso, Cote d'Ivoire, Cambodia, Georgia, Paraguay, Peru, Senegal, and Turkey (business sector).

For 2004-2005, there are ongoing activities related to cyber security technologies for e-applications in Afghanistan, Azerbaijan, Barbados, Bhutan, Bulgaria (Phase III), Bulgaria (Phase II), Cameroon, Jamaica, Rwanda, Turkey (for e-health and e-government), and Zambia (for e-signatures).

# ITU-D's mandate for security - *Activities*

| WSIS Plan of Action, Dec 2003 | Reference to ITU WTDC, March 2002 (Istanbul - Programme 3) |
|---|---|
| b) Governments in cooperation with the private sector, should prevent, detect and respond to cybercrime and misuse of ICTs.<br>c) Governments, and other stakeholders, should actively promote user education and awareness about online privacy/means of protecting privacy.<br>d) Take appropriate action on spam at national and international levels.<br>e) Encourage the domestic assessment of national law with a view to overcoming any obstacles to the effective use of electronic documents and transactions including electronic means of authentication. | Through IsAP3 provide assistance to Member States in developing laws and model legislation for e-services/ applications, prevention of cybercrime, security, ethical issues and data privacy. |

**II ) Legislation**

*Assisting in the formulation of appropriate legislation*

Providing assistance to countries in the elaboration of model legislation, covering areas such as electronic commerce, data protection, online transactions, digital certification, authentication and encryption. Countries involved: ASETA Member States (Bolivia, Columbia, Ecuador, Peru and Venezuela) Burkina Faso, Cape Verde, Mauritania, Mongolia and Tanzania.

Activities are planned for the Pacific Island States notably Cook Islands for 2005.

# ITU-D's mandate for security - *Activities*

| WSIS Plan of Action, Dec 2003 | Reference to ITU WTDC, March 2002 (Istanbul - Programme 3) |
|---|---|
| f) Further strengthen the trust and security framework with complementary and mutually reinforcing initiatives in the fields of security in the use of ICTs. | Through IsAP3 identify security requirements and propose solutions for the development of secure IP infrastructure for e-services/applications on various types of networks |
| g) Share good practices in the field of information and network security and encourage their use by parties concerned.<br>h) Invite interested countries to set up focal points for real-time incident handling and response, and develop a cooperative network between these focal points for sharing information and technologies on incident response. | Develop tools to facilitate the exchange of best practices on IT security, legal issues related to the areas of activity of the IsAP3 Programme. |

**III ) Policy and Strategy formulation**

*Addressing national and regional policies and strategies related to cybersecurity*

Workshops organized to share information and best practices in security, trust technologies and e-business policies (128 countries involved). ITU has organized workshops/seminars addressing technology strategies for e-security in number of countries. Among others; Azerbaijan, Cameroon, Chile (for Mercosur), Mongolia, Pakistan, Paraguay, Romania, Seychelles, Syria, and Uzbekistan.

# ITU-D's mandate for security - *Activities*

| WSIS Plan of Action, Dec 2003 | Reference to ITU WTDC, March 2002 (Istanbul - Programme 3) |
|---|---|
| i) Encourage further development of secure and reliable applications to facilitate online transactions.<br>j) Encourage interested parties to contribute actively to the ongoing UN activities to build confidence and security in the use of ICTs. | It is necessary to address the security concerns in order to leverage the potentials of public networks as vehicles for delivering affordable value-added e-services/ applications. |

**III) Policy and Strategy formulation (continued)**
*Addressing national and regional policies and strategies related to cybersecurity*
Security and trust were amongst the main topics discussed at the November 2004 ITU Regional e-government and IP symposium for the Arab Region which resulted in the Dubai Declaration emphasising the need for continued ITU activities in cybersecurity for e-applications and services.

For 2005, workshop to address cybersecurity in Europe, CIS, CEE, and the Baltic States where topics such as identity management, spam, cyber crime, data confidentiality and national information security policies were addressed. Others include this event, and ITU WSIS Thematic Meeting on Cybersecurity.

# ITU-D's mandate for security - *Funding*

- Funding for ITU-D projects 2004-2005 related to cybersecurity.
- **Working with governments and funding entities** is key.
- Activities have been and continue to be funded by ITU partners and governments.
  - The Inter-American Development Bank is funding a project in Jamaica while the Communications Authority of Zambia is **funding the related security and trust platform**.
  - The European Community is providing 85% of the **funding for projects** in Cameroon and Rwanda.
  - The Government of Turkey and the World Bank are **funding e-transformation and e-government projects** for Turkey.

International Telecommunications Unit

# ITU-D's mandate for security - *Actions*

- **Activities to create tools and guidelines for the countries**

  → Objective: to develop tools for addressing security and trust issues and guidelines for the successful implementation of e-application projects

- **Activities to assist ITU members**

  → The goal is to increase the participation of developing country experts and solution providers in project implementation and increase activities aimed at addressing e-application cybersecurity issues.

  - regional seminars;
  - assistance in elaborating strategies for e-security for e-government;
  - ICT symposia addressing IP, applications and security issues;
  - workshops on cybersecurity for ICT networks.

International Telecommunications Unit

# I. Sample project – **Georgia**

## – *Securing communication within government networks*

**Challenge:** Government of Georgia project to convert paper documents (including restricted ones) into digital format to facilitate dissemination of government information to citizens. Officials plan to electronically sign official correspondences. **How** can access to these documents be controlled? **How** can integrity of official electronic correspondence be ensured?

**Solution:** Implementation of public key infrastructure (PKI) providing strong certificate-based authentication including fingerprint biometrics, data integrity using digest algorithms, e-signature and data confidentiality based on both public key and symmetric encryption. Solutions built on existing infrastructure to ensure seamless integration. Funding and implementation by ITU.

International Telecommunications Unit

# I. Sample project – **Paraguay**

## – *Securing the transmission of sensitive documents*

**Challenge:** Clients of CONATEL needed to secure IT solutions to transmit confidential data to CONATEL. To address this requirement, the solutions had to ensure the integrity of data, preserve the confidential nature of the documents, and ensure that both sender and receiver are certain of the identities of each other.


S**olution:** ITU/BDT assisted in the design/development of a **public key infrastructure (PKI)** providing solutions for identity mgmt, non-repudiation, data integrity and strong encryption. Technology components including digital signature, biometric authentication, cryptographic token interface were built on existing infrastructure. Funded and implemented by ITU/BDT, this project has increased process efficiency, provides a secure and reliable solution for client communication.

International Telecommunications Unit

# I. Sample project – **Turkey**

## – *Building security and trust for the health sector*

**Challenge:** Connecting 81 provinces, 90,000 doctors, 1200 hospitals and 70+ million inhabitants to be through an ICT health platform as part of **national health transformation project**. Technological, policy, regulatory and institutional challenges, and **security and trust issues** to be addressed. (Transmission of medical records, authenticating doctors, patients, healthcare professionals and institutions, ensuring confidentiality, integrity, privacy and ownership of EPRs and protecting critical infrastructure and data. )

**Solution** (Phase I): Secure health info system enabling citizens, medical institutions, health insurance and health care professionals to use ITU to store/access/disseminate sensitive health data national wide. Funding by Government of Turkey. Coordination and implementation by ITU.

# I. Sample project – **Bulgaria**

## – *Building security & confidence in government services*

**Challenge:** Securing communication between government officials and providing security for IP-based interconnection of government agencies. Main challenges included providing solutions for authentication, data integrity, data confidentiality and non-repudiation.


**Solution:** **Phase I** provided solutions for certificate-based authentication of government officials, confidentiality in the transmission of sensitive documents and non-repudiation through e-signatures. In **Phase II** three government agencies were interconnected using **PKI-enabled Virtual Private Networks** as a cost-efficient way to use the Internet for sensitive e-government services. Project funding and coordinating the design and implementation was provided by ITU/BDT.

International Telecommunications Unit

# I. Other ongoing projects

– ***Barbados, Cameroon, Jamaica, Rwanda and Zambia***

**Challenges:** Enabling secure transaction-based e-government services, such as renewing national IDs online, obtaining land certificates, securing the transmission of documents between government officials and agencies, providing online payment for government services and interconnecting government agencies using PKI-enabled Virtual Private Networks.

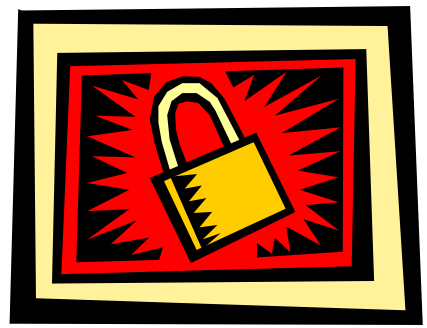
**Solutions:** e-signatures, data confidentiality and integrity, as well as finger print biometrics.
Funding by host governments, EU and ITU. Implementation by ITU.

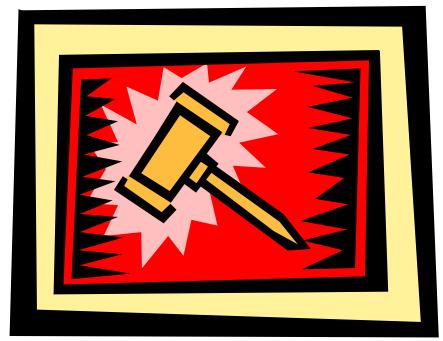
International Telecommunications Unit

# II. Legislative framework for e-appl.

***- Including data privacy and data protection***

Assisted **ASETA** (Bolivia, Colombia, Ecuador, Peru and Venezuela) to develop a harmonized legal framework for the delivery of services based on digital certification, e-signature and e-commerce, data privacy and consumer protection for e-transactions.



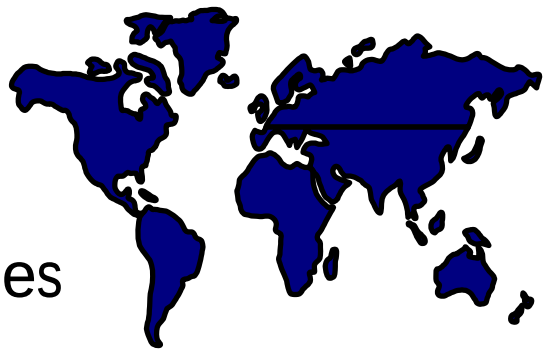


International Telecommunications Unit

# II. Building security awareness

***- Providing assistance for national policies***

**Sub-regional seminar** for Caribbean countries in St. Lucia to discuss sub-regional strategies for e-legislation.



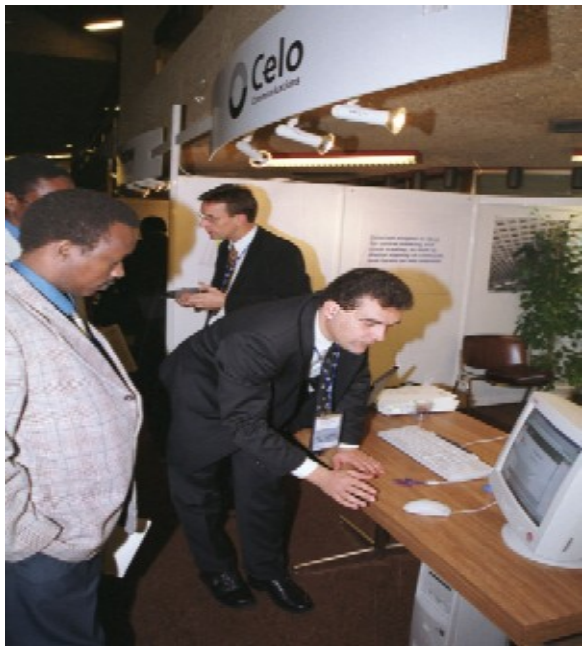
**Workshops and seminars** addressing technology strategies for cybersecurity for e-applications in Azerbaijan, Cameroon, Chile, Mongolia, Pakistan, Paraguay, Romania, Seychelles, Syria and Uzbekistan.

International Telecommunications Unit

# III. Increase security awareness

## *- Workshops & seminars for strategy development*

Over 500 participants from 128 countries, including 50 security experts from IT security companies, met at ITU HQ to launch a technology strategy for building trust and security for e-business transactions.




**African delegate participating in a live PKI demonstration**

Delegates from developing country had the opportunity to see an operational PKI, participate in live demonstrations and gain an understanding of some of the technology issues, challenges and solutions in place.

**Delegates at workshop**

International Telecommunications Unit

# Summary of ITU-D activities for 2005

1. **PKI Projects:** Barbados, Cameroon, Jamaica, Rwanda, Turkey and Zambia.
   New request for ITU assistance from Seychelles.

2. **Seminars and Workshops:** Cybersecurity Seminar for CEE, CIS and the Baltic States. Cybersecurity Seminar for Latin America. ITU WSIS Thematic Meeting on Cybersecurity in Geneva in collaboration with ITU-T and the ITU Strategy and Policy Unit.

3. **Publications:** Internet Protocol Policy Manual in collaboration with ITU-T. Guidelines for the implementation of E-Health Projects.
   **Cybersecurity Manual for Developing Countries**

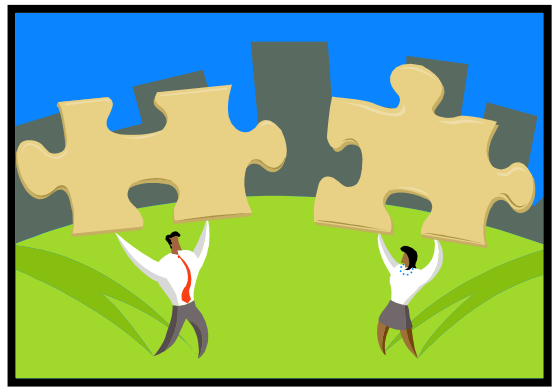
International Telecommunications Unit

# Way forward for cybersecurity

International Telecommunications Unit

# Next steps for cybersecurity

- Building confidence and security in the use of ICTs are crucial elements in further developing the Information Society.
- Provide forum for regulators to discuss issues, challenges and threats.
- Help developing countries formulate legislation for combating spam and building cybersecurity.



- Need for greater coordination of national Internet security initiatives and for enhanced international cooperation in combating viruses, and fighting cybercrime.
- Promote the development of a multilateral agreement on cooperation against spam and towards global cybersecurity

International Telecommunications Unit

# Recent ITU cybersecurity events

- **ITU/ EU (ENISA) Regional Seminar on Cybersecurity**
  *Riga, Latvia, May 2005*
  Within the framework of its mandate in the Istanbul Action Plan Programme 3, ITU-D and the Government of Latvia organized a seminar on cybersecurity for CIS, CEE and Baltic States.

- **ITU-T Cybersecurity Symposium II**
  *Moscow, Russian Federation, March 2005*
  Held on the first day of the Russian Association for Networks and Services Conference on Security to highlight the importance of cybersecurity as an essential part of ICTs.

- **ITU-T Cybersecurity Symposium I**
  *Florianópolis, Brazil, October 2004*
  The first ITU-T Cybersecurity Symposium, held the day before ITU's annual World Telecommunication Standardization Assembly, to cover some of the most important issues facing network operators, enterprises, governments and individuals today and explain how ITU-T can help to make **cyberworld a safer place.**

International Telecommunications Unit

# Recent ITU cybersecurity events

- **ITU WSIS Thematic Meeting on Countering Spam**
  *Geneva, Switzerland, July 2004*
  WSIS Thematic Meeting organized in the framework of the implementation of the WSIS Declaration of Principles/Action Plan.

- **ITU Global Symposium for Regulators (GSR)**
  *Geneva, Switzerland, December 2003*
  Sharing views and best practices in regulation. Discussion on frame-works for international cooperation on cybersecurity and spam.

- **ITU-T Workshop on Security**
  *Seoul, Republic of Korea, May 2002*
  Discussions on network security issues and possible technical solutions.

- **Creating Trust in Critical Network Infrastructures**
  *Seoul, Republic of Korea, May 2002*
  Looked at the policy and regulatory implications of network infrastructures and areas for international cooperation.

International Telecommunications Unit

# Thematic Meeting on Cybersecurity

- Held between 28 June and 1 July 2005 at ITU headquarters in Geneva, Switzerland.
- Jointly organized by ITU-D, ITU-T and the ITU Strategy and Policy Unit
- The meeting will examine the recommendations in the WSIS Declaration of Principles and Plan of Action relating to **building confidence and security** in the use of ICTs and the **promotion of a global culture of cybersecurity.**
- The meeting will focus on six broad themes in promoting international cooperative measures among governments, the private sector and other stakeholders.

*For more information, see the event website at:*
*www.itu.int/cybersecurity/*

International Telecommunications Unit

# Final remarks

- International governmental and private sector approach needed and justified by seriousness of threat.
- Collective security approach needed because of global interdependencies.
- No single government or any single forum can address all cooperation issues.

- Despite there not being one approach that works under all conditions, the sharing of good practices in the fields of information and network security, encouraging there usage by all parties, is crucial for success.
- **ITU stands ready to assist wherever it can!**

International Telecommunications Unit

# Thank you

International Telecommunication Union

Helping the world communicate

International Telecommunications Unit

# Links

ITU activities related to cybersecurity:
www.itu.int/cybersecurity

ITU activities on countering spam:

www.itu.int/spam

WTSA resolutions 2004:

www.itu.int/ITU-T/wtsa/resolutions04/

ITU-D and E-strategies:

www.itu.int/ITU-D/e-strategies

Anti-spam laws and authorities worldwide:
www.itu.int/osg/spu/spam/law.html

ITU WSIS thematic meeting on spam material:
www.itu.int/osg/spu/spam/background.html

World Summit on the Information Society:

www.itu.int/wsis

International Telecommunications Unit