Building Confidence and Security in the Use of ICTs and the International Cooperation Agenda

UNITAR / Intel Training Session on "Information Security: A Policy Perspective"

UN Headquarters, New York
30 August 2006

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

Agenda

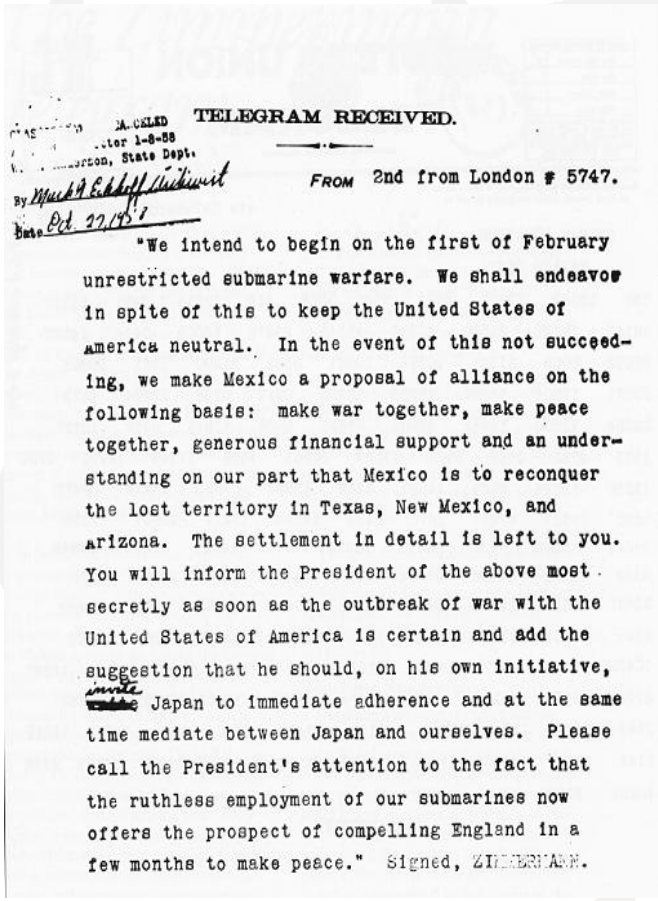
- Trust and Confidence Issues in Communications: a New Problem?
- Security in the Context of the WSIS
- ITU, WSIS, and Cybersecurity
- The International Cooperation Agenda
  - Security-related Activities and Meetings
  - Case study: Spam in the Larger Context of Cybersecurity
- The Importance of Awareness Raising
  - The Roles of Governments, Businesses, Citizens, and International Organizations
  - Introducing Five Main Themes in Cybersecurity
  - ITU Cybersecurity Gateway
  - Cybersecurity in the Context of Developing Countries
- Next Steps in Achieving Global Cybersecurity

Trust and Confidence Issues in Communications: a New Problem?

Examples from the Past

- Intercepts and hacks of the **telegraph** played an important role in the past.
- There are lessons to be learned also from this...

A Famous Telegram in 1917



TELEGRAM RECEIVED.

...ter 1-8-58
...rton, State Dept.
By ...
Date Oct. 22,'58

FROM 2nd from London # 5747.

"We intend to begin on the first of February unrestricted submarine warfare. We shall endeavor in spite of this to keep the United States of America neutral. In the event of this not succeeding, we make Mexico a proposal of alliance on the following basis: make war together, make peace together, generous financial support and an understanding on our part that Mexico is to reconquer the lost territory in Texas, New Mexico, and Arizona. The settlement in detail is left to you. You will inform the President of the above most secretly as soon as the outbreak of war with the United States of America is certain and add the suggestion that he should, on his own initiative, invite Japan to immediate adherence and at the same time mediate between Japan and ourselves. Please call the President's attention to the fact that the ruthless employment of our submarines now offers the prospect of compelling England in a few months to make peace." Signed, ZIMMERMANN.

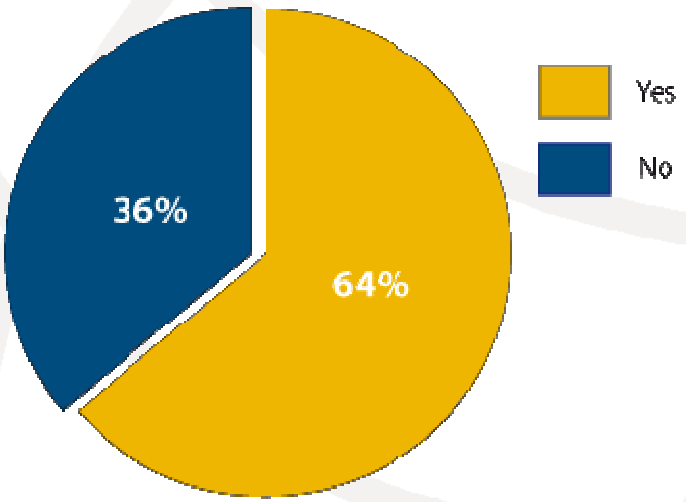
- The **Zimmerman Telegram** (displayed in decrypted form) played a major role in the United States entering World War I.
- The **telegram** was decrypted by British Intelligence

ITU Cybersecurity Trust and Awareness Survey 2006

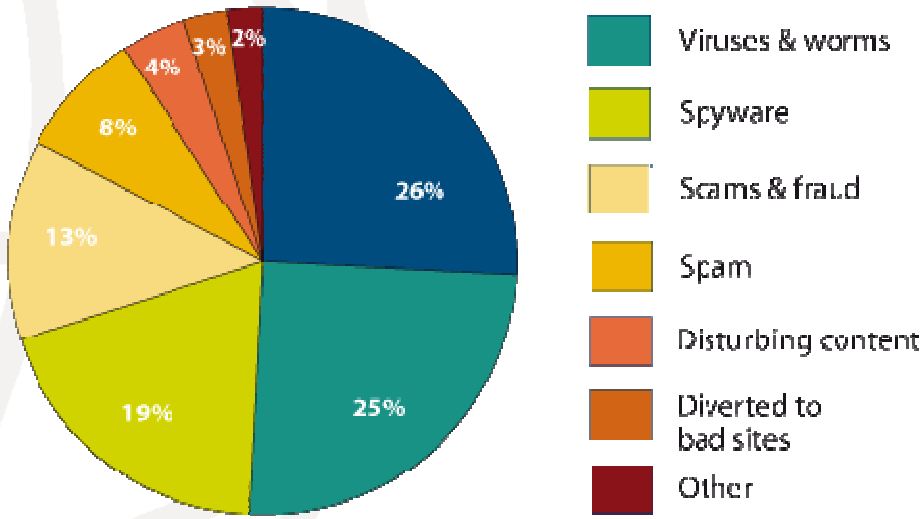
Online Fears

Responses to an online survey, March May 2006

Do you avoid certain activities online for security concerns?



What is your greatest online fear



Source: ITU Trust and Awareness Survey 2006

Setting the Context

- In the 21st century, there is a **growing dependency** on information and communications systems (ICTs) that span the globe;
- **Rapid growth in ICTs** and dependencies led to shift in perception of cybersecurity threats in mid-1990s;
- Linkage of cybersecurity and critical infrastructure protection (CIIP);
- A number of countries began assessment of threats, vulnerabilities and explored mechanisms to redress them;
- After national consideration, began move to international political agenda;
- **At World Summit on the Information Society (WSIS), "Building confidence and security in the use of ICTs" emerged as one of the "key principles" for building an inclusive Information Society**

Recent Developments

- *4 August 2006* Announcement: " **U.S. Senate Ratifies Council of Europe (CoE) Convention on Cybercrime** "
  - *The convention targets hackers, those spreading destructive computer viruses, those using the Internet for the sexual exploitation of children or the distribution of racist material and terrorists attempting to attack infrastructure facilities or financial institutions.*
  - *The Convention is in full accord with all U.S. constitutional protections, such as free speech and other civil liberties, and will require no change to U.S. laws.*

- *18 August 2006 News Article*: " **ISPs Wary About 'Drastic Obligations' on Web Site Blocking** "
  - *"EU officials want to shutter suspicious websites as part of a 6-point plan to boost joint antiterrorism activities."*
  - *EC VP wants to block websites that incite terrorist action.*
  - *"Because it's unclear what ministers actually mean by 'tackling the use of the Internet,' the European Internet Services Providers Association said it couldn't comment on the announcement."*
  - *"It also underlines once again that 'monitoring calls, Internet and e-mail traffic for law enforcement purposes is a task vested in the government,' which must reimburse carriers and providers for retaining the data".*

News sources: The Associated Press and Warren's Washington Internet Daily 2006.

Cybersecurity and the International Cooperation Agenda

International Cooperation Agenda

- **Council of Europe Cybercrime Convention** (1997-2001)
  - First international treaty seeking to address internet crimes by harmonizing national laws, improving investigative techniques and increasing cooperation among nations.
  - 40+ countries have ratified the Convention to date.
- UN Resolutions 55/63 (2000) and 56/121 (2001) related to Combatting the criminal misuse of information technologies;
- **UN Resolutions 57/239 (2002) and 58/199 (2004): Creation of a global culture of cybersecurity and the protection of critical information infrastructure;**
- ITU Plenipotentiary Resolution 130 (2002): Strengthening the role of ITU in information and communication network security;
- WSIS Phase I (2003): Chapter 5 in Declaration of Principles and Plan of Action: Building confidence and security in the use of ICTs
- WSIS Phase II (2005): Tunis Commitment (paras 15 and 24) and Tunis Agenda: Part C on Internet Governance (paras 39-47, 57-58, 68);

Etc.

International Cooperation Agenda

- WSIS Thematic Meeting on Countering Spam (2004);
- ITU WSIS Thematic Meeting on Cybersecurity (2005);
- ITU World Telecommunication Development Conference (WTDC) Resolution 45 (Doha, 2006): Mechanisms for enhancing cooperation on cybersecurity, including combating spam;
- **Further cybersecurity discussions to take place at ITU Plenipotentiary Conference, November 2006 (Antalya, Turkey)**

WSIS Outcomes: Building Confidence and Security in the Use of ICTs

World Summit on the Information Society (WSIS)

- WSIS proposed by Tunisia at ITU Plenipotentiary Conference in 1998. Adopted as UN Summit in 2001
- First Phase, Geneva, 10-12 December 2003
  - **11'000 participants**, of which 41 Heads of State/Govt
  - Adopted **Geneva Declaration** & **Plan of Action**
- Second Phase, Tunis, 16-18 November 2005
  - **25'000 participants**, of which 47 Heads of State/Govt
  - Adopted **Tunis Commitment** & **Agenda for Information Society**
  - Focus on Internet Governance and Financing of ICT4D

world summit on the information society
Geneva 2003 - Tunis 2005

Security-related Excerpts from the WSIS Documents

Building confidence and security in the use of ICTs is a necessary pillar in building a global information society.

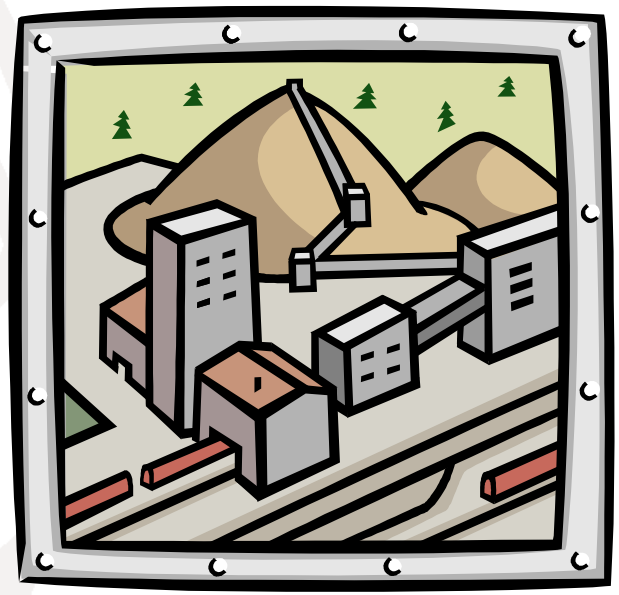
- References to "Building Confidence and Security in the use of ICTs":
  - **Chapter 5** in WSIS 2003 **Declaration of Principles** and **Plan of Action**
  - Extracts from WSIS 2005 **Tunis Commitment** and **Tunis Agenda**

- *Highlighting:*
  - Critical information infrastructure protection
  - Promotion of a global culture of cybersecurity
  - Harmonizing national legal approaches, international 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

Critical Information Infrastructure Protection

From WSIS Phase II: *Tunis Commitment*

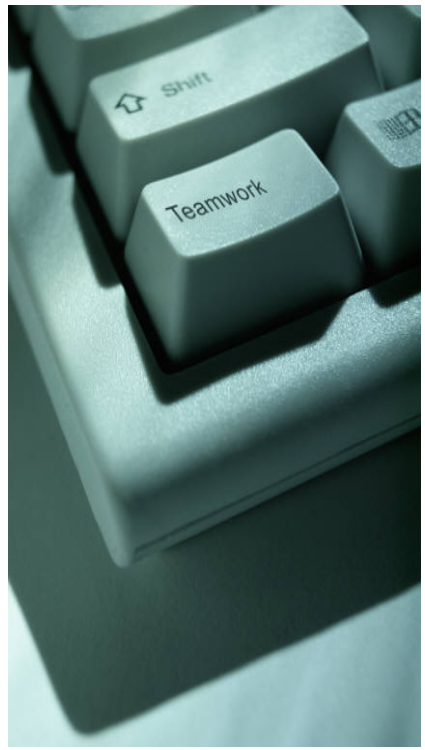
15. ***We further recognize*** *the need to effectively confront challenges and threats resulting from the use of ICTs for purposes that are inconsistent with objectives of maintaining international stability and security and may adversely affect the integrity of the infrastructure within States, to the detriment of their security. It is necessary to prevent the abuse of information resources and technologies for criminal and terrorist purposes, while respecting human rights.*



Promotion of Global Culture of Cybersecurity

From WSIS Phase II: *Tunis Agenda*

39. *We seek to build confidence and security in the use of ICTs by **strengthening the trust framework.** We reaffirm the necessity to further promote, develop and implement in cooperation with all stakeholders a global culture of cybersecurity, as outlined in UNGA Resolution 57/239 and other relevant regional frameworks. This culture requires national action and increased international cooperation to strengthen security while enhancing the protection of personal information, privacy and data. **Continued development of the culture of cybersecurity** should enhance access and trade and must take into account the level of social and economic development of each country and respect the development-oriented aspects of the Information Society.*

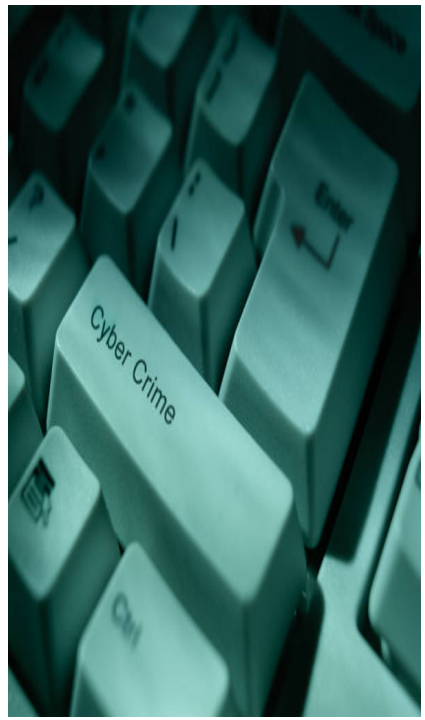


Harmonizing National Legal Approaches, International Legal Coordination & Enforcement

From WSIS Phase II: *Tunis Agenda*

40. ***We underline the importance of the prosecution of cybercrime, including cybercrime committed in one jurisdiction, but having effects in another.*** *We further underline the necessity of effective and efficient tools and actions, at national and international levels, to promote international cooperation among, inter alia, law enforcement agencies on cybercrime.*

We call upon governments in cooperation with other stakeholders to develop necessary legislation for the investigation and prosecution of cybercrime, noting existing frameworks, for example, UNGA Resolutions 55/63 and 56/121 on Combatting the criminal misuse of information technologies and regional initiatives including, but not limited to, the Council of Europe's Convention on Cybercrime.



Countering Spam

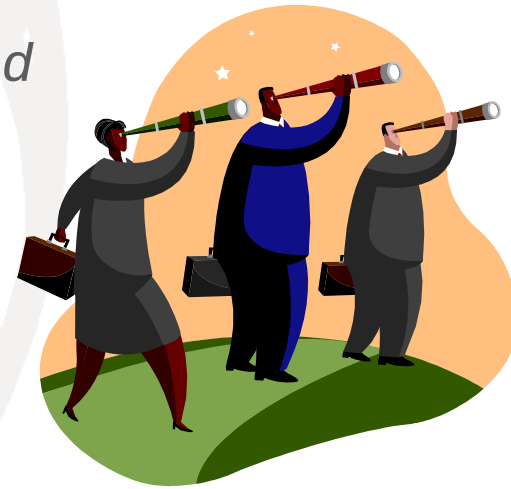
From WSIS Phase II: *Tunis Agenda*

*41. We resolve to **deal effectively with the significant and growing problem posed by spam.** We take note of current multilateral, multi-stakeholder frameworks for regional and international cooperation on spam, for example, the APEC Anti-Spam Strategy, the London Action Plan, the Seoul Melbourne Anti-Spam Memorandum of Understanding and the relevant activities of OECD and ITU. We call upon all stakeholders, to adopt a multi-pronged approach to counter spam that includes, inter alia, consumer and business education; appropriate legislation, law enforcement authorities and tools; the continued development of technical and self-regulatory measures; best practices; and international cooperation.*

Developing Watch, Warning and Incident Response Capabilities

From WSIS Phase I: *Plan of Action*

C5 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.*



Information Sharing of National Approaches, Good Practices and Guidelines

From WSIS Phase II: *Tunis Agenda*

45. We underline the ***importance of the security, continuity and stability of the Internet, and the need to protect the Internet and other ICT networks from threats and vulnerabilities****.*

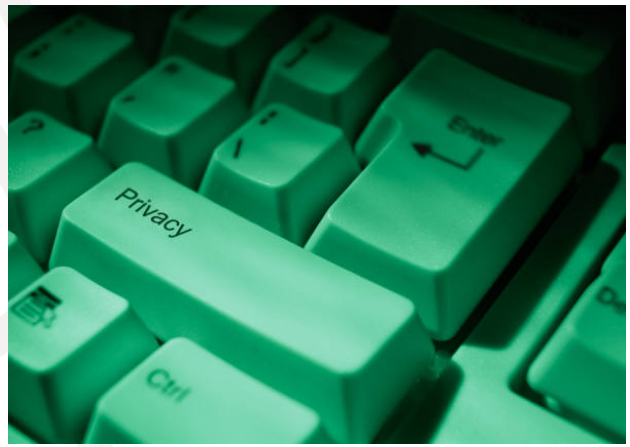
We affirm the need for a ***common understanding*** *of the issues of Internet security, and for* ***further cooperation*** *to facilitate outreach, the collection and dissemination of security-related information and exchange of good practice among all stakeholders on measures to combat security threats, at national and international levels*.

Privacy, Data and Consumer Protection

From WSIS Phase II: *Tunis Agenda*

46. ***We call upon all stakeholders to ensure respect for privacy and the protection of personal information and data, whether via adoption of legislation, the implementation of collaborative frameworks, best practices and self-regulatory and technological measures by business and users.***

We encourage all stakeholders, in particular governments, to reaffirm the right of individuals to access information according to Geneva Declaration of Principles and other mutually agreed relevant international instruments, and to coordinate internationally as appropriate.



ITU, WSIS and Cybersecurity

WSIS Action Lines and Facilitators

WSIS Action Lines	Focal Points
C1. The role of stakeholders	UN DESA
C2. Information and communication infrastructure	ITU
C3. Access to information and knowledge	UNESCO
C4. Capacity building	UNDP
C5. Building confidence and security in the use of ICTs	ITU
C6. Enabling environment	UNDP
C7. ICT Applications	
• E-government	UN DESA
• E-business	UNCTAD
• E-learning	UNESCO
• E-health	WHO
• E-employment	ILO
• E-environment	WMO
• E-agriculture	FAO
• E-science	UNESCO
C8. Cultural diversity and identity, linguistic diversity and local content	UNESCO
C9. Media	UNESCO
C10. Ethical dimensions of the Information Society	UNESCO
C11. International and regional cooperation	UN DESA

ITU, WSIS, and Cybersecurity

- ITU is an international organization within the United Nations System where **governments and the private sector** coordinate global telecom networks and services. Founded in 1865, it is oldest specialized agency of the UN system. ITU has 190 Member States, 780 Sector Members & Sector Associates.
- ITU Resolution 130 (2002) put emphasis on strengthening the role of the ITU in information and communication network security.
- ITU World Telecommunication Standardization (2004) Resolutions, include:
  - Resolution 50 on “Cybersecurity”
  - Resolution 51 on “Combating spam”
  - Resolution 52 on “Countering spam by technical means”
- There are currently more than seventy ITU recommendations focusing on security.
- ITU World Telecommunication Development Conference (2006) Resolutions, include:
  - Resolution 45 on Mechanisms for enhancing cooperation on cybersecurity, including combating spam

Case Study: Spam in the LARGER Context of Cybersecurity

What have we Learned from the Work on Spam to Date?

- International cooperation and coordinated action is crucial;
- Technology provides solutions but a multi-layered policy approach must continue to be employed;
- Global rollout of legislation and enforcement regimes is effective in containing spam;
- Need enforcement action to bring wrongdoers into line and send signals to professional spammers;
- Support and engagement of **industry** will contribute to better outcomes;
- **Spam is now one of the more prominent risks to internet security and has rapidly mutated from a general annoyance to a broader cybersecurity threat.**

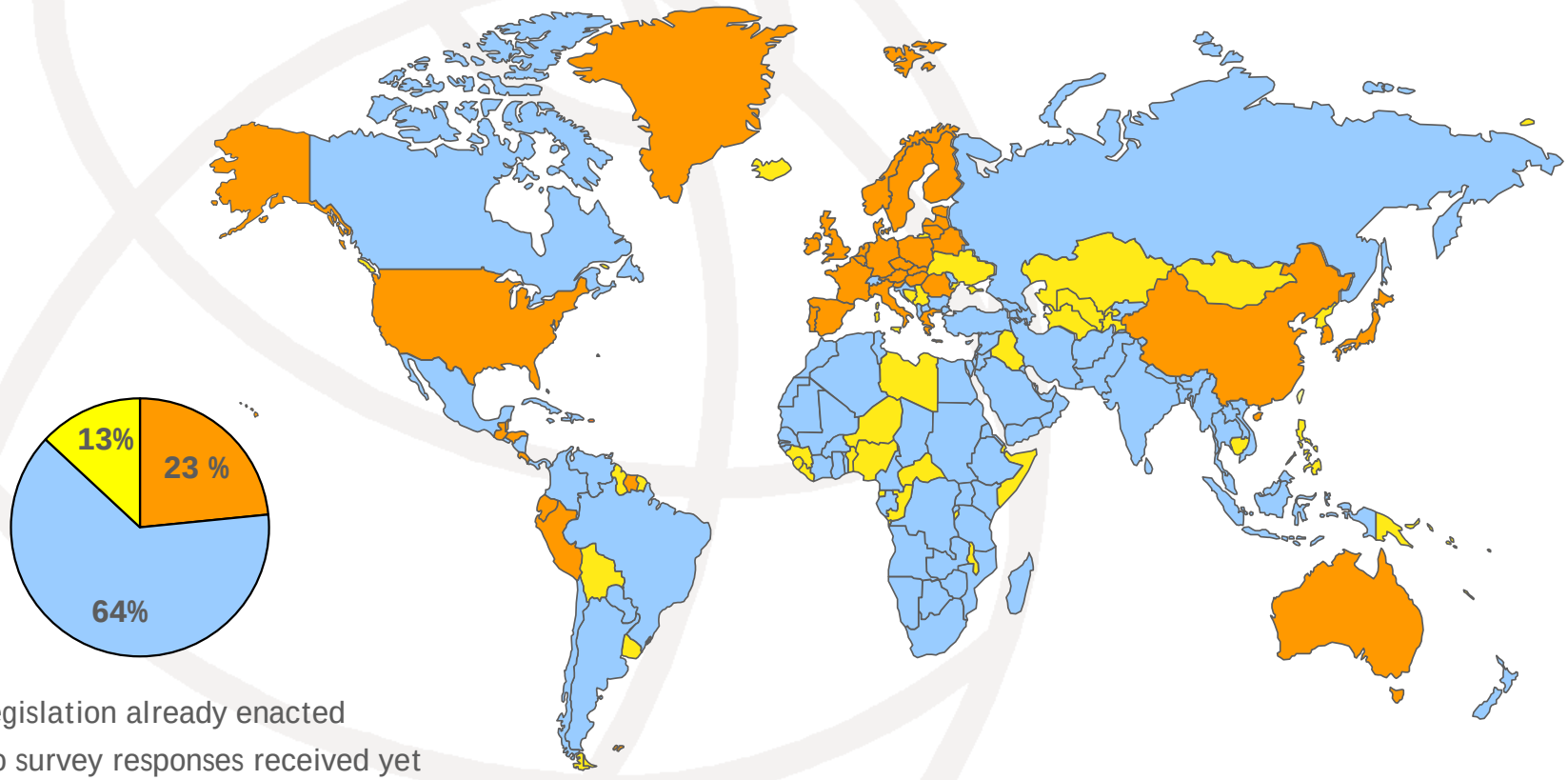
*Text includes some direct input from ACMA in Australia

Some Spam-related Issues and Solutions Industry is Currently Discussing

- International cooperation;
- Private sector partnerships;
- Technology;
- Legislation & regulation;
- Education & awareness raising

Picture source: Messaging Anti-Abuse Working Group; http://www.maawg.org /

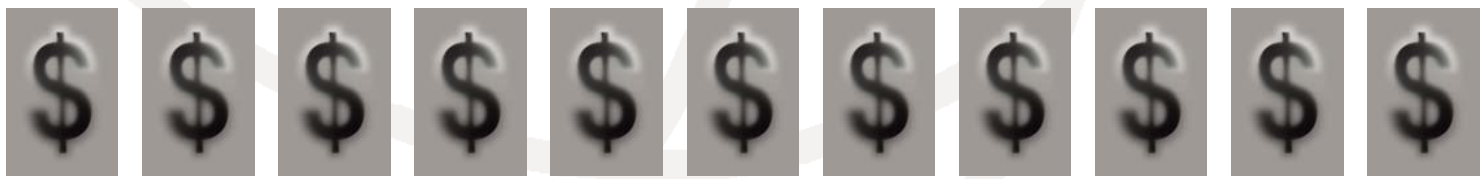
ITU Survey on Spam Legislation (2005)



Note: The boundaries and names shown and the designations used on this map do not imply official endorsement or acceptance by the United Nations.

Laws & Legislation to Fight Spam?

- Anti-spam measures require well-conceived, targeted, and coordinated **enforcement mechanisms** in order to be effective.
- ***Challenge:*** anti-spam investigations are invariably complicated and expensive
- ***As a result:*** developing countries that have limited resources for such work, anti-spam laws can be rendered nearly meaningless…



A Multi-layered Approach to Countering Spam

- Spam is a global problem that requires a multi-layered comprehensive approach that includes:
  - **Effective legislation and enforcement**
  - Development of **technical measures**
  - Establishment of industry **partnerships and self-regulation**
  - **Education** (and awareness raising)
  - **International cooperation** (as spam can originate anywhere to be sent to a receiver located in any country, city, around the globe)
- Spam activities need to be considered in the **larger context of cybersecurity**, on-line crime and other malicious use of the online environment.

Past Security-related Activities in the Context of WSIS

Past Cybersecurity-related Meetings

- **WSIS Thematic Meeting on Countering Spam**

  Focus: Defining spam and different approaches to countering spam

  - A multi-pronged approach to dealing with spam is an appropriate measure.

- **ITU WSIS Thematic Meeting on Cybersecurity**

  Focus: Five cybersecurity themes and cybersecurity in the context of developing countries

  - Understanding the complexity of the cybersecurity issue and that a multi-layers approach is needed for the larger cybersecurity issues: collaboration is key moving forward.

- ***First WSIS Action Line C5 Facilitation Meeting: Building Confidence and Security in the Use of ICTs***

  Focus: Cybersecurity in the context of WSIS and next steps

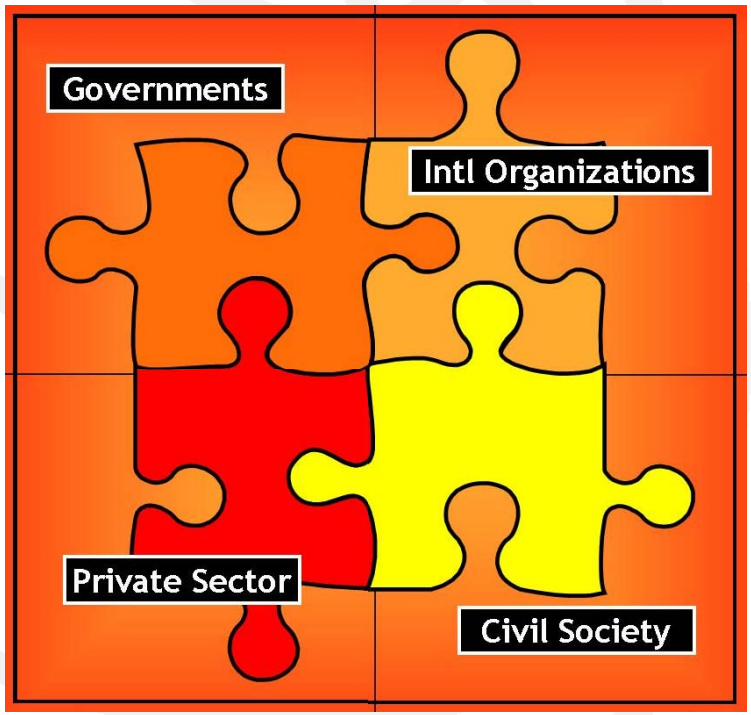
  - Follow-up on the WSIS Implementation Mechanism
  - Framework for Partnerships for Global Cybersecurity
  - Three proposed areas for **collaboration** and focused **capacity building**

Initial Consultation Meeting for WSIS Action Line C5

- ITU is the focal point for facilitating Action Line C5.
- Meeting organized at ITU Headquarters in Geneva, Switzerland, from **15-16 May 2006**.
- Meeting organized in conjunction with World Telecommunication Day 2006 which had the theme "*Promoting Global Cybersecurity*".
- In today's interconnected world of global networks, threats can originate anywhere: national, regional, international cooperation is paramount to promoting, developing and implementing a global culture of cybersecurity.
- **The necessity of building partnerships across themes and stakeholders is clearly evident for Action Line C5.**

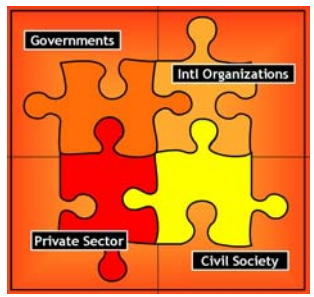
Website: http://www.itu.int/osg/spu/cybersecurity/2006/index.phtml

Roles of the Different Stakeholders in Cybersecurity



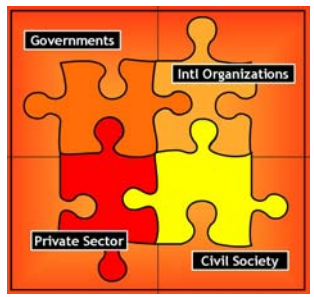
Role of Government / Public Sector

- Each nation's government must determine the level of **cybersecurity risk** that it is willing to accept and expose its citizens and businesses to.
- It is the responsibility of each government to ensure that the country is ready and capable of protecting its own citizens and by doing so contribute the building a global culture of cybersecurity.
- The **strategy** that the government employs for information and network security impacts the country's economic and social development, and international competitiveness.
- **The government needs to clearly distribute roles and related responsibilities to ensure that the structure they have built ensures relative cybersecurity on the national level and does not leave any gaps and uncovered areas.**



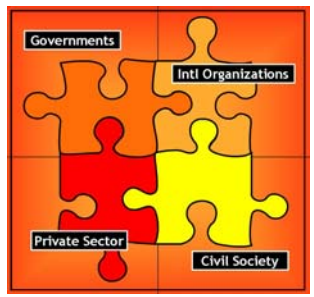
Role of Businesses / Private Sector

- Responsibilities and role related to the ownership of information and communication infrastructures.
- Example: In many countries it is the private sector that is the first to act on the rapid technological development that are constantly taking place, as they need as they need to assess the impact and opportunities this may involve for the company specifically.
- As effective security requires an in-depth understanding of the various aspects of information and communication networks, the **private sector's expertise should be increasingly involved in the development and implementation of a country's cybersecurity strategy**



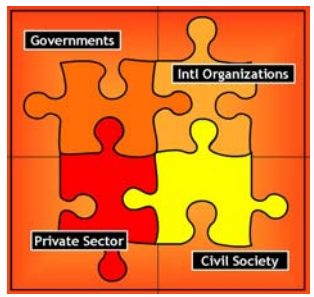
Role of Citizens/Civil Society

- The average user is not adequately educated to understand the threats and how to protect himself/herself.
- It is the responsibility of each user to become aware of the threats as well as the opportunities that connectivity presents them with.
- The users and consumers also have specific expectations on the kind of service they receive and how much they are willing to pay for these services.
- Due to the interconnected features of information and communication technologies, security overall can only be fully promoted when the **users have full awareness** of the existing threats and dangers. Governments, businesses, and the international community must therefore proactively **help users access information on how to protect themselves**.



Role of Intl. Organizations

- Organizations in the international community have a special role in sharing information on good practices, and creating open and accessible fora for the **exchange of ideas and extensive collaboration.**
- **International cooperation** at the levels of government, industry, consumer, business, technical groups, to allow a global and coordinated approach to achieving global cybersecurity **is key**.



What's Next for WSIS Action Line C5?

- C5 encompasses a broad range of *themes* and *actors*.
- Challenges include:
  - Getting the different parties to talk to each other
  - Getting the parties to collaborate in order to reduce transaction costs, duplication of work, etc.
  - **Developing countries** face unique challenges in developing security policies and approaches appropriate to their circumstances.
- **In order to move forward there is a need to explore new partnerships among governments, the private sector, and other stakeholders.**

ITU Cybersecurity Gateway

(Launched 16 May 2006)

The Global Cybersecurity Gateway

http://www.itu.int/cybersecurity

Cybersecurity Gateway: Goal

- The goal of the Cybersecurity Gateway is to make stakeholders more aware of the various actors and groups working on the different areas of cybersecurity on the national, regional and international level.
- By providing an easy-to-use information resource on national, regional and international cybersecurity-related activities and initiatives worldwide.

Actors in Five Main Areas

I. Information sharing of national approaches, good practices and guidelines;

II. Developing watch, warning and incident response capabilities;

III. Technical standards and industry solutions;

IV. National legal approaches and international legal coordination and enforcement;

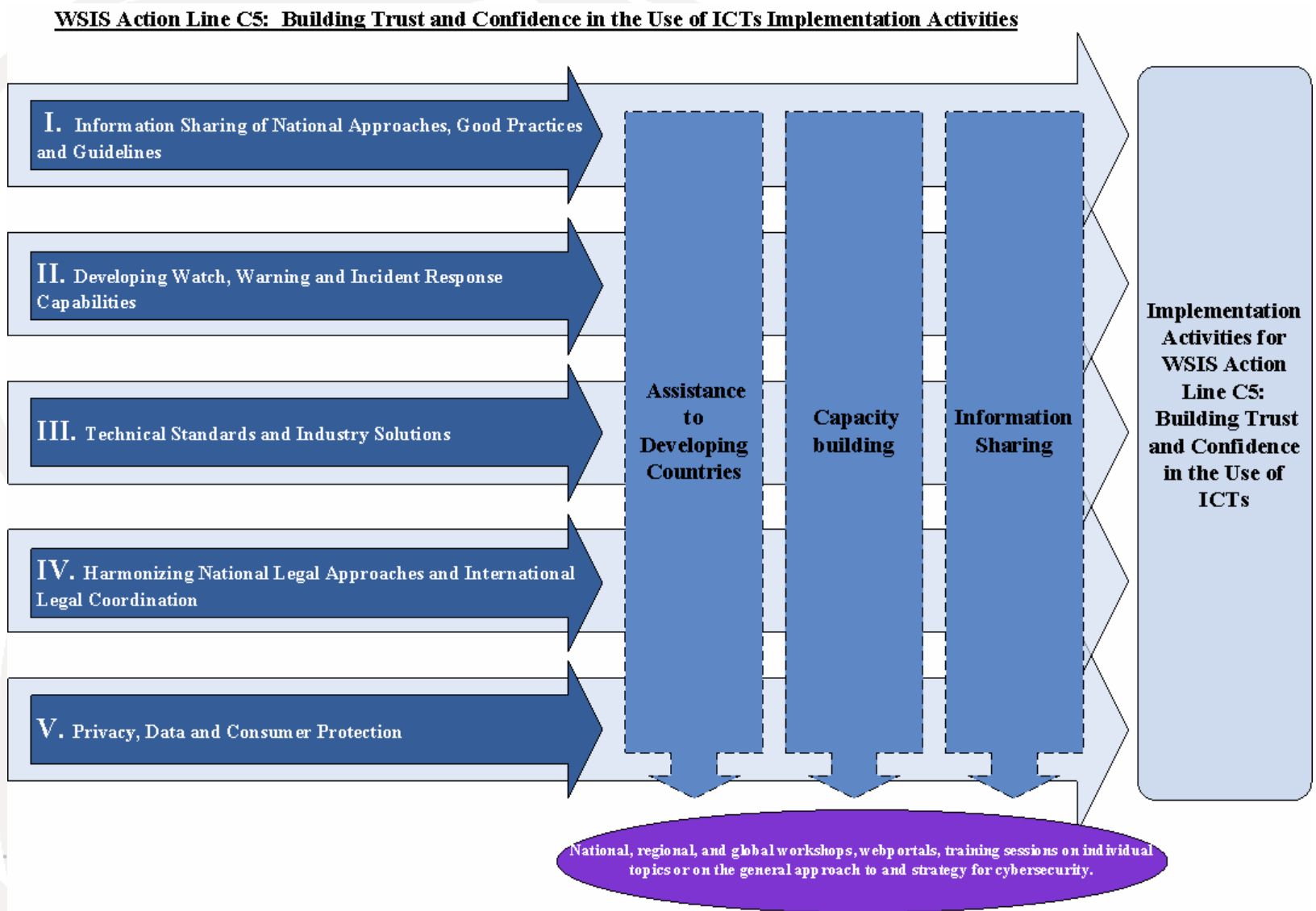
V. Privacy, data and consumer protection.

Structure of the Gateway

- The portal is geared towards four specific audiences: ***Citizens; Businesses; Governments, International Organizations***
- Database information collected within five main **themes**:
  1. Information sharing of national approaches, good practices and guidelines;
  2. Developing watch, warning and incident response capabilities;
  3. Technical standards and industry solutions;
  4. Harmonizing national legal approaches and international legal coordination and enforcement;
  5. Privacy, data and consumer protection.
- Additional information resources on the following **topics**: spam, spyware, phishing, scams and frauds, worms and viruses, denial of service attacks, etc.

Next Steps in Achieving Global Cybersecurity…

Overview of the WSIS Action Line C5 Landscape



Planned Activities for Action Line C5

1) ***Focus Area:*** **Information-sharing of national approaches, good practices and guidelines**

   Proposed activity**:** To further examine the common elements in various national approaches and develop a generic model framework or toolkit that national policy-makers could use to develop and implement a national cybersecurity or CIIP programme.

2) ***Focus Area:*** **Harmonizing national legal approaches and international legal coordination**

   Proposed activity**:** Capacity-building activities on the harmonization of cybercrime legislation, the Council of Europe's Convention on Cybercrime, and enforcement.

3) ***Focus Area:*** **Developing watch, warning and incident response capabilities**

   Proposed activity**:** Extended information sharing of best practices on developing watch, warning and incident response capabilities.

Upcoming Security-related Meetings

- ITU-D meeting related to ITU Resolution 45 on "**Mechanisms for enhancing cooperation on cybersecurity, including combating spam**" *(31 August - 1 September 2006)*
- **First Meeting of the Internet Governance Forum (IGF)** *(30 October-2 November 2006)*
  - One of the four thematic focus areas will consider "Security-Creating trust and confidence through collaboration"
- ITU Meeting at World Telecom in Hong Kong focusing on the "**Countering spam cooperation agenda**" *(8 December 2006)*
- **Annual meetings** for progress on WSIS Action Line C5 "Building confidence and security in the use of ICTs" *(May 2007, TBC)*

Quotes from Speaker at First WSIS Action Line C5 Meeting

"No single nation can successfully secure itself in isolation"

"Each nation's security is limited by that of the **weakest link** in the global infrastructure"

"There is a need for national action and international cooperation to build a global culture of cybersecurity."

"It is critical to **build awareness at a national policy level** of the importance of cyber/critical information infrastructure protection."

"**If government leads, the private sector, individuals and SMEs will follow**. Once the national government has a **plan** and **strategy** in place, they should reach out regionally and internationally to find out how they can best interact with their counterparts elsewhere."

(Michele Markoff, Senior Coordinator for International Critical Infrastructure Protection with the Bureau of Political Military Affairs, U.S. State Department)

Thank you for your attention

International Telecommunication Union

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

Information Resources and Links

- **Cybersecurity Gateway: http://www.itu.int/cybersecurity**
- Collected ITU security-related resources: http://www.itu.int/cybersecurity/itu_activities.html
- Some ITU resolutions and initiatives related to cybersecurity: http://www.itu.int/osg/spu/cybersecurity/ituevents.html
- Chairman's Report, Facilitation Meeting for WSIS Action Line C5 (2006): http://www.itu.int/osg/spu/cybersecurity/2006/chairmansreport.pdf
- Chairman's Report, ITU WSIS Thematic Meeting on Cybersecurity (2005): http://www.itu.int/osg/spu/cybersecurity/chairmansreport.pdf
- Chairman's Report, WSIS Thematic Meeting on Spam (2004): http://www.itu.int/osg/spu/spam/chairman-report.pdf
- ITU Resolution 45 (Doha 2006): Mechanisms for enhancing cooperation on cybersecurity, including combating spam http://www.itu.int/ITU-D/e-strategy/cybersecurity/index.html
- Internet Governance Forum (IGF) http://www.intgovforum.org/
- ITU Newslog category dedicated to security: http://www.itu.int/osg/spu/newslog/CategoryView,category,Cybersecurity.aspx