WSIS Outcomes: Building confidence and security in the use of ICTs

WSIS Action Line C5 Facilitation Meeting: “Promoting Global Cybersecurity”

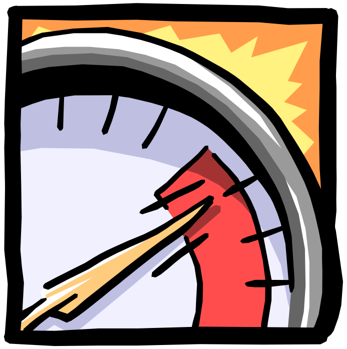
15-16 May 2006

Robert Shaw
Deputy Head
ITU Strategy and Policy Unit

Agenda

- Setting the Context
- International Cooperation Agenda
- World Telecommunication Day/World Information Society Day
- Some Key Challenges
- Possible Themed Approach
- Outcomes from the WSIS Documents

Setting the Context



- In the 21st century, growing dependency on information and communications systems (ICTs) that span the globe;
- Rapid growth on 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 WSIS, “Building confidence and security in the use of ICTs” emerged as one of the “key principles” for building an inclusive Information Society

Example: “Zombie Botnets”

- Exploit used to hijack millions of private computers, by infecting them with viruses, worms or trojans, turning each infected machine into an anonymous proxy (zombie) under “bad guy” control;
- Since early 2003, almost all viruses have been created and sent out by spammers in order to build giant networks of hijacked machines through which to send their spam (zombie botnets);
- Today, 50-70% of spam now sent by zombie botnets;
- Spamhaus has list of ~four million infected machines: 60,000 to 100,000 new infections per week;
- Zombie botnets, besides relaying spam, are also being used to launch Distributed Denial of Service (DDOS) attacks
  - e.g. used to blackmail online gambling sites & banks, small-scale cyberwarfare among states

International Cooperation Agenda

- Council of Europe Cybercrime Convention (1997-2001).
- 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*;

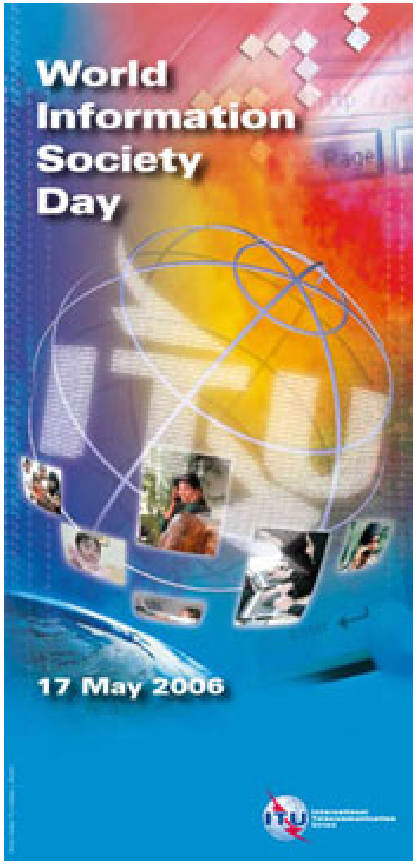
International Cooperation Agenda

- WSIS Thematic Meeting on Countering Spam (2004);
- ITU WTSA Resolution 50 (2004): Cybersecurity;
- WSIS Thematic Meeting on Cybersecurity (2005);
- WSIS Phase II (2005): Tunis Commitment (para 15, 24) and Tunis Agenda: Part C on Internet Governance (paras 39-47, 57-58, 68);
- WTDC Resolution 45: (Doha, 2006): Mechanisms for enhancing cooperation on cybersecurity, including combating spam;
- ITU Plenipotentiary Conference November 2006? (Antalya, Turkey).

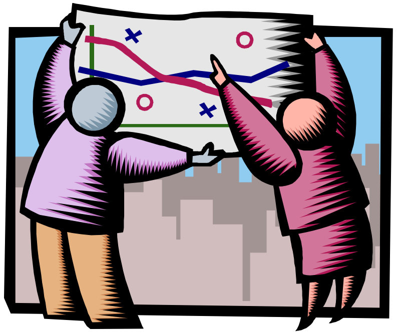
- Many more examples….

Background: World Telecommunication Day/ World Information Society Day

- WTD 2006 Theme: **Promoting Global Cybersecurity**
  - to highlight serious challenges we face in ensuring the safety and security of networked information and communication systems
- In *Tunis Agenda for the Information Society*, adopted at WSIS (November 2005), UNGA called upon to also designate 17 May as *World Information Society Day*
  - On 27 March 2006, UNGA adopted Resolution A/RES/60/252 proclaiming 17 May as annual World Information Society Day
- WTD 2006 *Promoting Global Cybersecurity* activities planned but after *Tunis Agenda* tasked ITU with C5 facilitation, combined initiatives



Some Key Challenges



- *"An undefined problem has an infinite number of solutions"*
  - Robert A. Humphrey
- Identifying and understanding key *themes*
- Identifying relevant *actors*
  - through survey, research (e.g. ITU Cybersecurity Gateway)
- Engaging 'siloed' communities who normally don't talk with each other
- *Creating platform for enhanced multistakeholder collaboration and partnerships*
  - with small "transaction costs"

A Themed Approach?

- Derived from the **2005 WSIS Thematic Meeting on Cybersecurity**
  - information sharing of national approaches, good practices and guidelines (particularly for developing economies);
  - developing watch, warning and incident response capabilities;
  - harmonizing national legal approaches, international legal coordination & enforcement;
  - industry solutions and technical standards;
  - privacy, data and consumer protection;
  - Other themes possible...

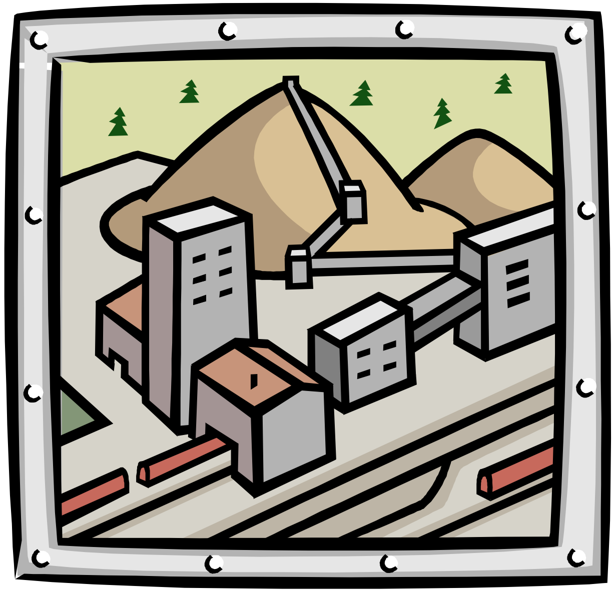
What do WSIS negotiated texts say about "Building confidence and security in the use of ICTs"?

- Chapter 5 in WSIS 2003 *Declaration of Principles* and *Plan of Action*
- Extracts from WSIS 2005 *Tunis Commitment* and *Tunis Agenda*

Critical Information Infrastructure Protection

From WSIS Phase II: *Tunis Commitment*

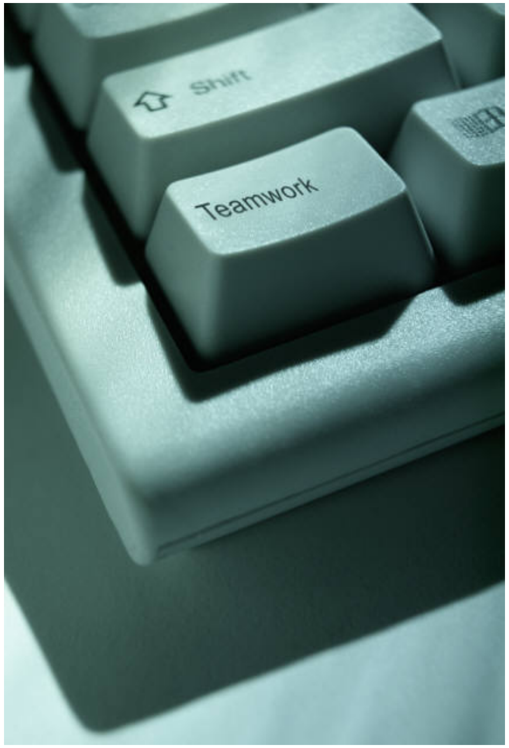
15. **We further recognize** the need to effectively confront challenges and threats resulting from the use of ICTs for purposes that are inconsistent with objectives of maintaining international stability and security and may adversely affect the integrity of the infrastructure within States, to the 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.

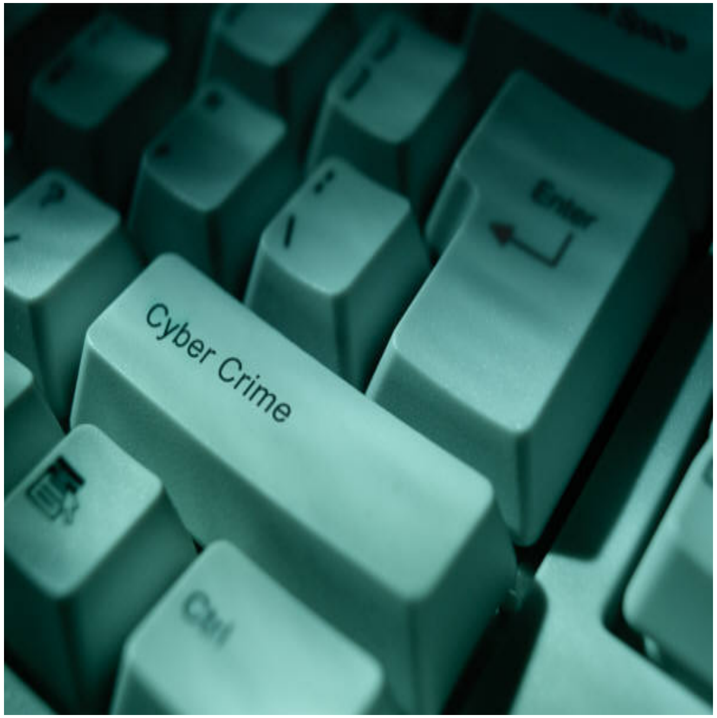


Harmonizing national legal approaches, international legal coordination & enforcement

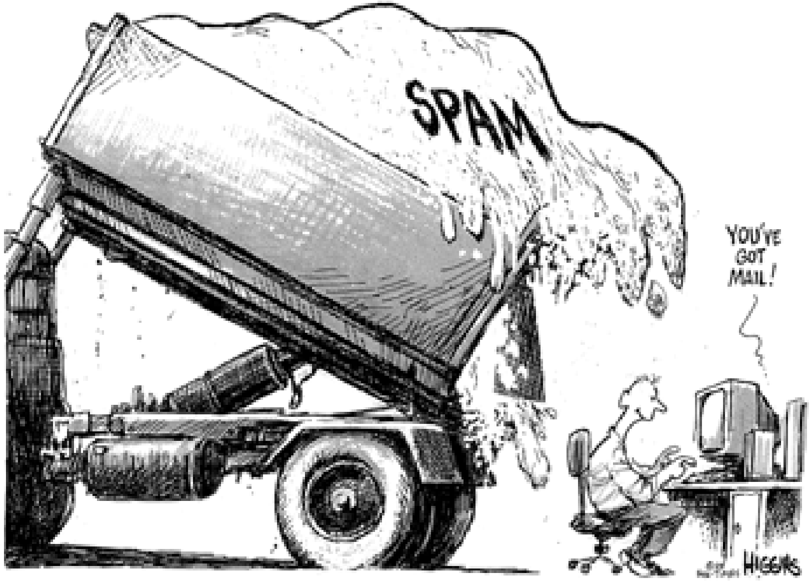
From WSIS Phase II: *Tunis Agenda*

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

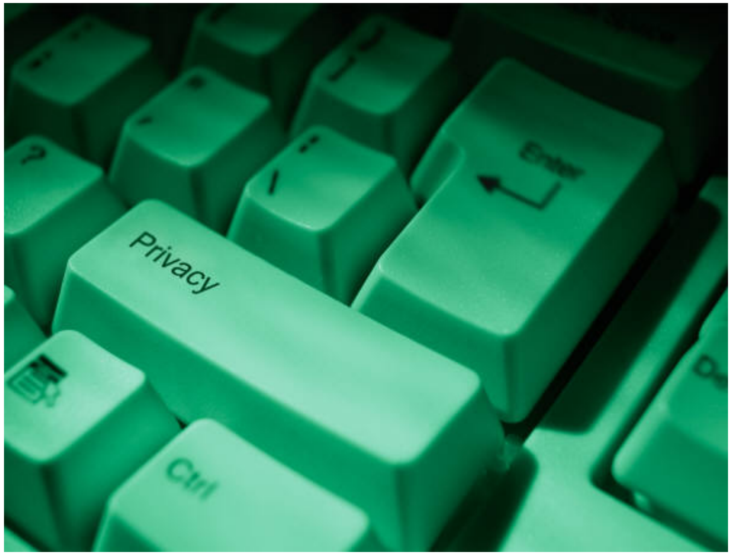
From WSIS Phase II: *Tunis Agenda*

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.



International Telecommunication Union

Building the Information Society