



**world summit
on the information society**
Geneva 2003 - Tunis 2005

Helping the world communicate



**International
Telecommunication
Union**

WSIS Thematic Meeting on Cybersecurity: Outcome and Next Steps

Global Symposium for Regulators
Hammamet, Tunisia
14 October 2005

Robert Shaw
ITU Internet Strategy and Policy Advisor
ITU Strategy and Policy Unit



14 November 2005

Global Symposium for Regulators



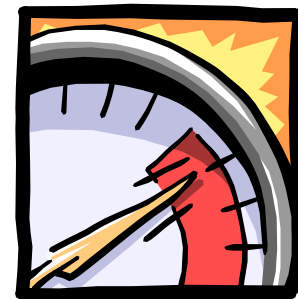
Agenda

- Setting the Context
 - Cybersecurity and Critical Infrastructure Protection
 - Common National Themes
 - International Cooperation Agenda
- ITU WSIS Thematic Meeting on Cybersecurity
 - Themes
 - Background papers
 - State of Play: Spam
- WSIS Phase II: Cybersecurity and Spam
- Some Possible Future ITU Activities



Setting the Context: Cybersecurity and Critical Infrastructure Protection

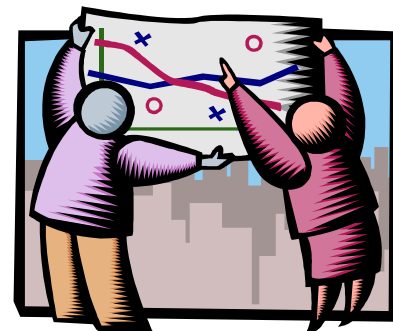
- In the 21st century, growing dependency on information and communications systems (ICTs) that span the globe;
- Rapid growth on ICTs and dependencies led to shift in perception of cybersecurity threats in mid-1990s;
- Linkage of cybersecurity and critical infrastructure protection;
- A number of countries began assessment of threats, vulnerabilities and explored mechanisms to redress them.





Common National Themes

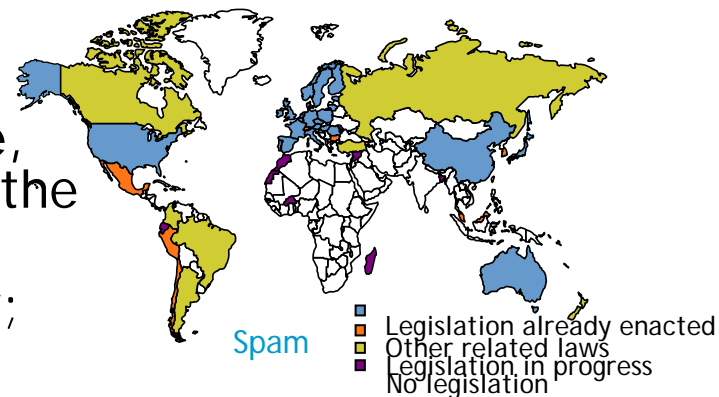
- Identification of what constitutes critical infrastructure sectors and risk assessment;
- Interagency and multi-stakeholder approach;
- Public-private partnerships identified as critical;
- Watch, warning and incident response capabilities built or enhanced;
- Review of national legal frameworks to enhance enforcement and judicial cooperation;
- Enhancement of privacy, data and consumer protection;
- Recognition of need to enhance international cooperation agenda.





International Cooperation Agenda

- WTDC and ITU PP 2006?
- WSIS Phase II (2005): Internet Governance, 3b) Public Policy Issues Related to Use of the Internet;
- WTSA Resolution 50 (2004): Cybersecurity;
- WSIS Phase I (2003) DoP: 5) and PoA C5.
Building confidence and security in the use of ICTs;
- ITU PP Res 130 (2002): Strengthening the role of ITU in information and communication network security;
- UN Resolutions 58/199 (2004) and 57/239 (2002): Creation of a global culture of cybersecurity and the protection of critical information infrastructure;
- Council of Europe Cybercrime Convention (1997-2001).



WSIS Thematic Meeting on Cybersecurity

28 June - 1 July 2005

- In framework of its activities to implement WSIS Plan of Action 2003), ITU hosted a **WSIS Thematic Meeting on Cybersecurity**;
- <http://www.itu.int/cybersecurity/> provides links to agenda, background papers, presentations, electronic contributions, Chairman's Report and complete audio archives;
- CD-ROM provides materials from both 2004 Countering Spam and 2005 Cybersecurity/Spam Thematic Meetings as well as a related materials from ITU's daily work programme on these topics.



Thematic Meeting on Cybersecurity

■ Six broad themes

- information sharing of national approaches, good practices and guidelines;
- developing watch, warning and incident response capabilities;
- harmonizing national legal approaches and international legal coordination;
- technical standards;
- privacy, data and consumer protection;
- providing assistance to developing economies.

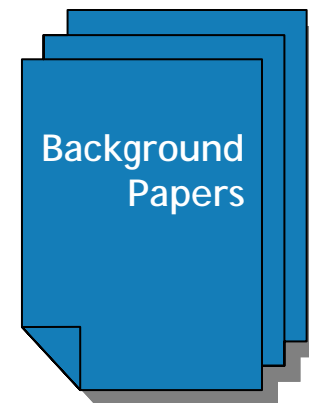
■ June 28: Countering Spam Day

- Considered developments since June 2004
WSIS Thematic Meeting on Countering Spam





Meeting background papers



- [A Comparative Analysis of Spam Laws: the Quest for Model Law](#): Derek BAMBAUER, John PALFREY, David ABRAMS, Berkman Center for Internet & Society, Harvard Law School, USA;
- [A Comparative Analysis of Cybersecurity Initiatives Worldwide](#): Myriam DUNN, Head, Center for Security Studies (CSS), Swiss Federal Institute of Technology, Switzerland;
- [Harmonizing National Legal Approaches on Cybercrime](#): Stein SCHJOLBERG, Chief Judge, Moss District Court, Norway & Amanda HUBBARD, Trial Attorney, Computer Crime and Intellectual Property Division, Department of Justice, USA;
- [ITU Survey on Anti-Spam Legislation Worldwide](#): Cristina BUETI, Strategy and Policy Unit (SPU), International Telecommunication Union



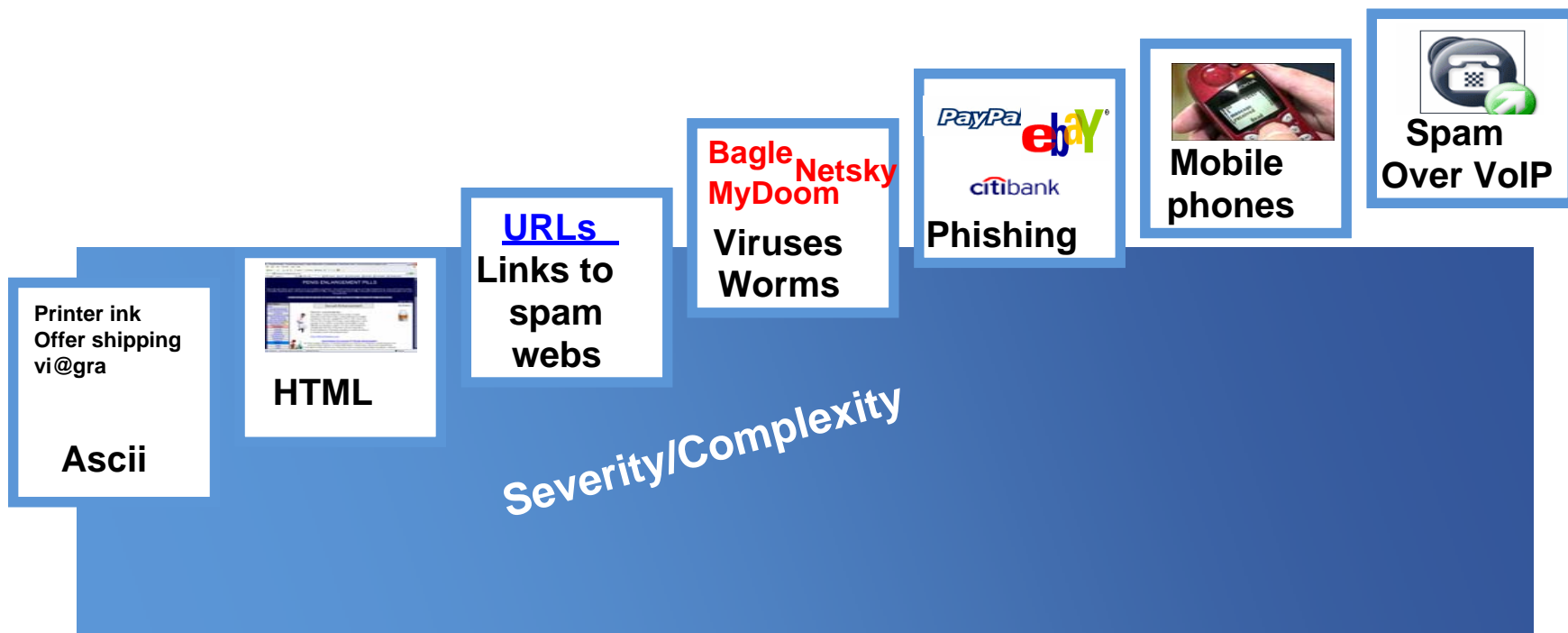
State of Play: Spam

- No clear consensus as to whether we are winning or losing war on spam;
- Spam under constant mutation from annoyance to general cybersecurity threat;
- Threat vector shifting to new platforms such as mobile and Voice over Internet Protocol (VoIP) networks;
- Spam should be considered in broader policy and regulatory context of “unwanted or unsolicited communications” without regard to platform.





Spam: Mutation from Annoyance to General Cybersecurity Threat



→ 2001 → 2005 → 2006 →





Example: “Zombie Botnets”



- Main exploit now used by spammers is hijacking millions of private computers, by infecting them with viruses, worms or trojans, turning each infected machine into an anonymous proxy (**zombie**) under the control of the spammer;
- 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



WSIS Phase II: Cybersecurity and Spam

- Chapter Three: Internet Governance, 3b) Public Policy Issues Related to the Use of the Internet
 - *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 cyber-security, 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 cyber-security 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. (Agreed)*





WSIS Phase II: Cybersecurity and Spam

- Chapter Three: Internet Governance, 3b) Public Policy Issues Related to the Use of the Internet
 - *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. (Agreed)*





WSIS Phase II: Cybersecurity and Spam

- Chapter Three: Internet Governance, 3b) Public Policy Issues Related to the Use of the Internet
 - *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 the 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. (Agreed)*
- Note there is nothing in this multi-pronged approach that cannot be argued to apply more generally to promoting global cybersecurity





Possible ITU Future Activities

- Survey, describe and raise awareness of issues faced by national policy makers in addressing cybersecurity:
 - Development of best practices, standards, technical guidelines and procedures to reduce vulnerabilities
 - National coordination mechanisms
 - Appropriate national legal infrastructures
 - Watch, warning and recovery capabilities
 - Government/industry partnerships
 - Outreach to civil society and consumers





Closing Remarks

- Each May 17th, ITU celebrates **World Telecommunication Day**, which celebrates ITU's founding in 1865 and its history of "helping the world communicate"
- According to the draft *Tunis Compact*, to be agreed at WSIS Tunis, the 17th May will henceforth be celebrated as World Information Society Day;
- **Promoting Global Cybersecurity** is 2006 theme:
 - ITU plans related awareness-raising campaign
 - Formulating our ideas and welcome your input on how we can best promote this message...





Links and References

- ITU Activities related to Cybersecurity and Thematic Meeting
 - www.itu.int/cybersecurity
- ITU Activities on Countering Spam and Thematic Meeting
 - www.itu.int/spam
- ITU-T Activities on Spam (Study Group 17)
 - www.itu.int/ITU-T/studygroups/com17
- ITU-D Activities on Spam
 - www.itu.int/ITU-D/treg/
 - www.itu.int/ITU-D/e-strategies
- Anti-spam laws and authorities worldwide
 - <http://www.itu.int/osg/spu/spam/law.html>
- World Summit on the Information Society
 - www.itu.int/wsis

