Cybersecurity & Spam after WSIS: How MAAWG can help

MAAWG Brussels Meeting

27-29 June 2006

Robert Shaw
Deputy Head
ITU Strategy and Policy Unit
International Telecommunication Union

Setting the Context

- In the 21st century, nations have 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 & critical information infrastructure protection (CIIP);
- A number of countries began assessment of threats, vulnerabilities and explored mechanisms to redress them;
- With national consideration and realization that solutions cannot be just at national levels, move to international political agenda;

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 and Plan of Action
- Second Phase, Tunis, 16-18 November 2005
  - 25'000 participants, of which 47 Heads of State/Govt
  - Adopted Tunis Commitment and Agenda for Information Society
  - Internet Governance and Financing of ICT4D
- At WSIS, "**Building confidence and security in the use of ICTs**" emerged as one of the "key principles" for building an inclusive Information Society

International Cooperation Agenda

- Council of Europe Convention on Cybercrime (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;
- WSIS Thematic Meeting on Countering Spam (2004);
- ITU WTSA Resolution 50 (2004): Cybersecurity;
- WSIS Thematic Meeting on Cybersecurity (2005);

International Cooperation Agenda

- WSIS Phase II (2005): Tunis Commitment (para 15, 24) and Tunis Agenda: Part C on Internet Governance (see paras 39-47, 57-58, 68);
- WTDC Resolution 45: (Doha, 2006): Mechanisms for enhancing cooperation on cybersecurity, including combating spam
  - Meeting on Aug 31-Sept 1 2006
  - consideration of instrument, e.g., MoU on cybersecurity/spam cooperation?
- ITU Plenipotentiary Conference November 2006 (Antalya, Turkey)

WSIS on Spam

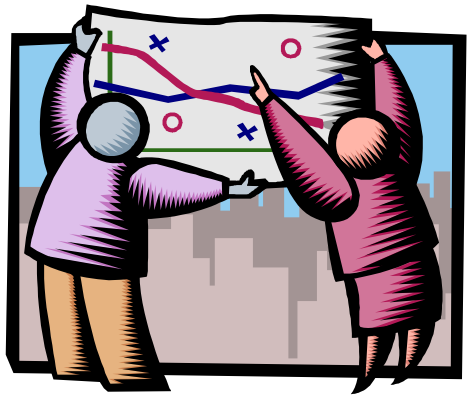
From WSIS Phase II: *Tunis Agenda*

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.

Post WSIS Activities Related to Cybersecurity and Spam

- 11 Action Lines for follow-up of WSIS with intergovernmental organizations acting as "facilitators" for partnerships and cooperation
- ITU is facilitator for WSIS Action Line C5: Building confidence and security in the use of ICTs
- Geneva: first C5 meeting held 15-16 May 2006
  - In conjunction with 17 May World Telecommunication Day theme of "Promoting Global Cybersecurity"
- Hong Kong: Dec 8 2006 meeting on spam (possibly linked with C5 activities)

Key Challenges



- Defining key *themes*
- Identifying relevant *actors*
- *Engaging* across 'siloed' communities who normally don't talk with each other
- Creating platform for multistakeholder *collaboration and partnerships*
- Likely first *deliverables*
  - Development of a cybersecurity/CIIP roadmap/toolkit for national policy makers
  - Capacity building on harmonization of cybercrime legislation, i.e., *COE Convention on Cybercrime*, enforcement
  - Assisting developing economies with implementation of watch, warning and incident response capabilities

ITU Cybersecurity Gateway attempts to Identify *themes*, *actors*, *topics*

Internet Governance Forum (IGF)

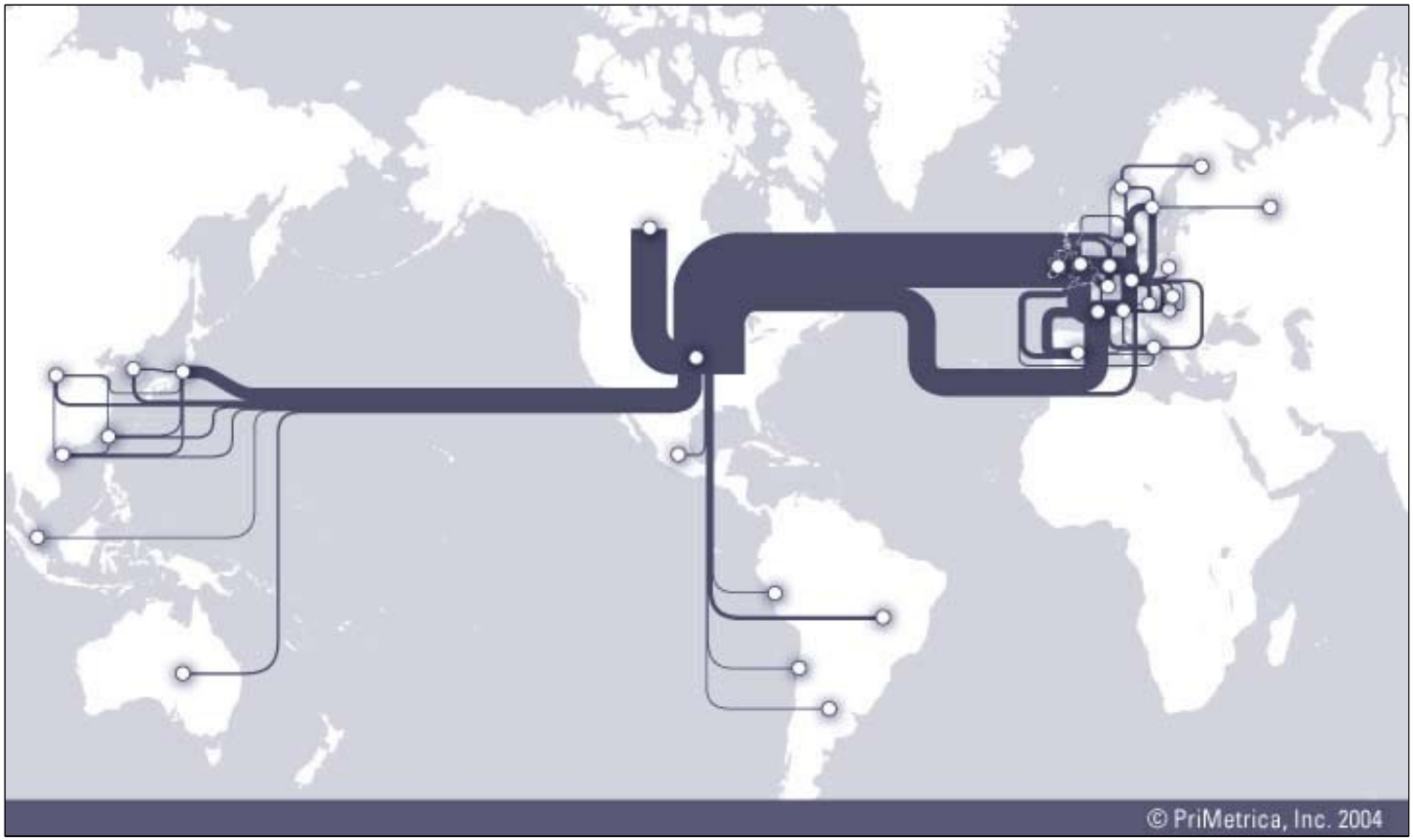
- See www.intgovforum.org
- First meeting in Athens, Greece: 30 Oct – 2 Nov 2006
  - (2007: Brazil, 2008: India)
- Annual information-sharing event with development focus: not decision-making forum
- 'Security' will be one plenary topic (~ 3 hours):
  - Building trust in an online environment;
  - Protecting users from spam, phishing, and viruses.
- OECD, ITU likely to organize workshops in Athens on spam and cybersecurity respectively

How MAAWG can help…

- Statistical studies are great help to policy makers (encouragement!)
- Cross participation on activities
  - WSIS C5 Follow-up
  - date coordination and joint initiatives…
  - e.g., MAAWG send representative to Dec 8 2006 meeting in Hong Kong (others: APCAUCE, OECD, APEC-TEL, ISC (China), ACMA, LAP, OFTA, tbd…)

How MAAWG can help cont'd…

- Consider perspective of developing economies



How MAAWG can help cont'd…

- Suggest best practice materials which might be of particular interest to developing economies
- Deliver tutorials to developing economies (or provide related tutorial materials)
  - high political pressure to do something proactive for developing economies…
- Other?

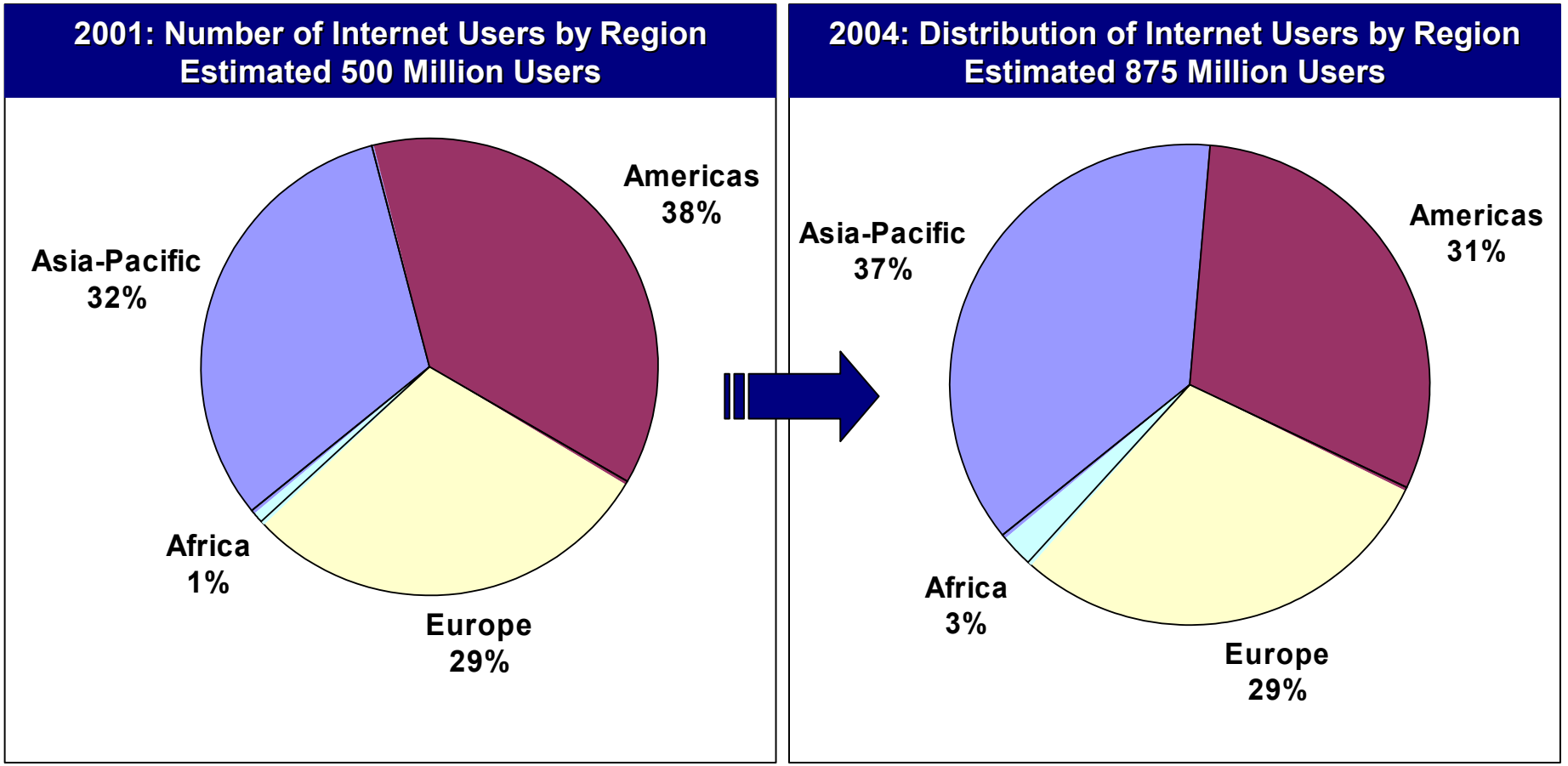
International Telecommunication Union

Building the Information Society

Extra Materials

Shift in Internet Demographics: Internet Users by Region 2001-2004

International Telecommunication Union



Asia-Pacific has overtaken Americas as largest percentage of regional Internet users with much more potential for growth…

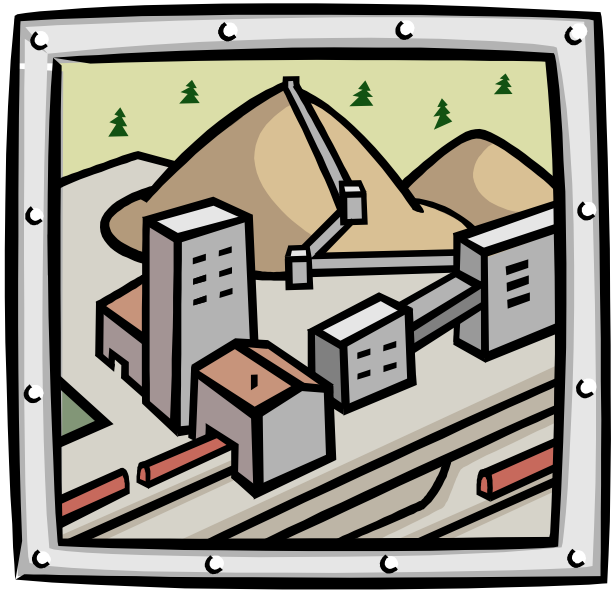
Additional Cybersecurity/Spam excerpts from WSIS Texts

see www.itu.int/wsis/

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*

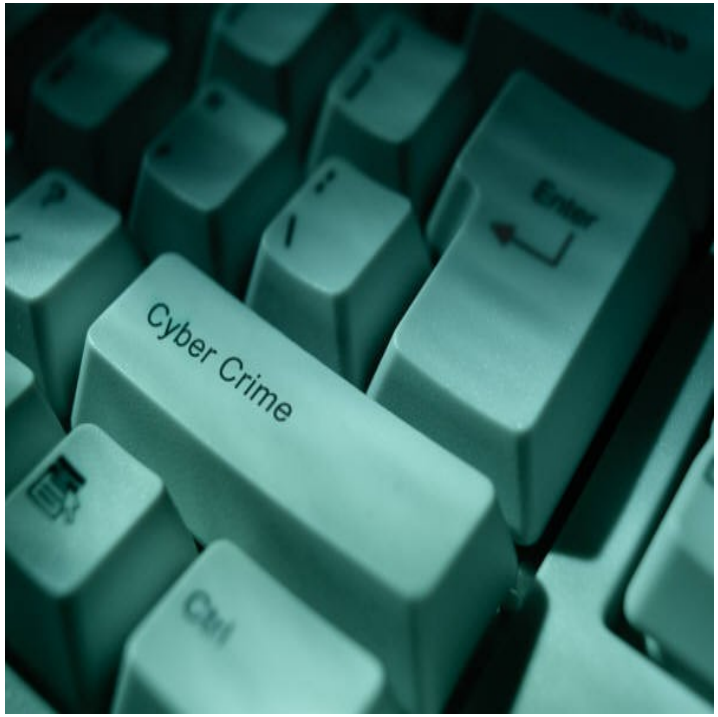
39. We seek to build confidence and security in the use of ICTs by strengthening the trust framework. We reaffirm the necessity to further promote, develop and implement in cooperation with all stakeholders a global culture of cybersecurity, as outlined in UNGA *Resolution 57/239* and other relevant 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.



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.