



MEETING ON MECHANISMS FOR COOPERATION
ON CYBERSECURITY AND COMBATING SPAM
31 August – 1 September 2006
ITU Headquarters Geneva (Room A)

MEETING REPORT

1. Introduction

WTDC2006 adopted Resolution 45 which called for the Director of the BDT to organize a meeting in conjunction with Doha Action Plan Programme 3 on mechanisms for cooperation on Cybersecurity and combating spam and to report to the 2006 ITU Plenipotentiary Conference the results of this meeting.

The meeting was opened by BDT Director Mr. Hamadoun TOURÉ who in his opening remarks stressed the importance of Cybersecurity, its broad scope and the importance for the meeting to arrive at concrete solutions that will address the needs of all membership taking into account specific challenges faced by developing countries and existing solutions.

Mr. Makhtar FALL of Senegal chaired the meeting assisted by Mr. Alexander NTOKO of BDT. The Chair presented the agenda which was adopted. In his opening remarks, the Chairman highlighted the challenges faced by developing countries in this domain and called for a spirit of collaboration and consensus to arrive at concrete results.

Some 50 participants including delegates from 24 Member States, Sector members, UN Office on Drugs and Crime, Council of Europe, European Commission, World Bank and ITU staff (BDT, TSB and General Secretariat) attended the two-day event. The meeting was organized in all six (6) ITU languages. For further information and background documents, please see <http://www.itu.int/ITU-D/cybersecurity>.

2. Presentation of input documents

The adoption of the agenda and opening remarks from the Chair were followed by a presentation by BDT on the mandate of the Development Sector in the domain of Cybersecurity and combating Spam. Other background and reference documents were used as sources for discussions and inspiration. Presentations on national, regional and multi-lateral and international initiatives on Cybersecurity and combating spam were made by Australia, Cisco Systems, Council of Europe, European Commission, Lithuania, Niger, Russian Federation, Sudan, Syrian Arab Republic on behalf of the Arab States, United Kingdom, United States of America, Uzbekistan and World Bank. The presentations highlighted initiatives in capacity building, legislation, technologies, incident response, policies and strategies, partnerships, and enforcement.

In addition to existing initiatives, new ones including proposals for the establishment of a Memorandum of Understanding were presented by delegates from developing countries. The contributions confirmed the existence of several initiatives most of them undertaken by developed countries with limited participation of developing countries.

3. Discussions and Analysis

Delegates commented on the presentations and made a several proposals on possible ways forward. The need for cooperation and collaboration was highlighted in most presentations and discussions. Delegates agreed on the necessity to leverage existing sources of expertise to meet the needs of developing countries. Most of the presentations and discussions identified areas where it was considered necessary for actions to be undertaken at the national, regional and international levels. Activities in capacity building, national legislation, national policies and strategies, public/private partnerships, enforcement mechanisms, information exchange, establishment of national focal points, incident response and technological solutions were identified as important for cooperation amongst Member States in cybersecurity and combating spam. There was a general agreement that it was

necessary for some mechanisms to be put in place to provide assistance to countries that requested it. During the discussions and analysis of the challenges¹ and existing initiatives, it was apparent that even though cyber threats and spam need to be addressed at a global level, the specific requirements especially those of developing countries have to be addressed. Participation of all interested countries (developing and developed) in a global and multi-lateral initiative would require all countries to meet some minimum national requirements in areas such as legislation, human and institutional capacity and appropriate national policies and strategies.

The presentations and discussions resulted in the identification of a number of areas where future activities should be undertaken by ITU-D to meet challenges faced by developing and least developed countries.

While many of the activities were to be undertaken at the national level, it was agreed that there was need for cooperation and coordination amongst the various stakeholders and initiatives and that ITU-D should play a role to facilitate the implementation of the actions that are part of its mandate and requested by Member States. It was suggested that certain practical tasks could be identified in this context and that ITU experience and expertise be utilized in undertaking them.

In line with the spirit and objective of Resolution 45, and considering the general agreement that some areas of activity needed coordination beyond existing frameworks, the main focus was now to agree on the type of mechanism to be put in place for ITU-D to provide the required assistance to developing countries. Three options were tabled for discussion.

- a. A memorandum of understanding amongst interested Member States with ITU Secretary-General as the depository.
- b. Technical cooperation framework(s) between ITU and interested Member States and partners.
- c. A project on the implementation of Resolution 45 for interested countries and with the participation of recognized sources of expertise.

All three options are aimed at putting in place mechanisms to enhance cooperation amongst interested stakeholders using expertise and experiences of existing entities and initiatives. All three options would be non-binding to Member States, open to interested countries and focused on addressing the needs of countries that are not part of existing frameworks.

One of the important considerations taken into account was the fact that ITU-D mandate in Cybersecurity and combating spam has in particular three main components – Doha Action Plan Programme 3, ITU-D Study Group 1 Question 22 and WTDC2006 Resolution 45. The output and recommendations made by this meeting were therefore aimed at proposals that were not already part of decisions agreed to by Membership at the WTDC2006 but to work towards mechanisms that were not part of existing decisions but necessary and requested by developing countries.

4. Recommendations for future actions

As a result of WSIS Thematic meeting on countering Spam, the following areas were considered important for the work in the domain of cybersecurity and combating spam.

1. Strong legislation
2. Development of technical measures
3. The establishment of industry partnerships, especially with Internet Service Providers, mobile carriers and direct marketing associations
4. The education of consumers and industry players about anti-spam measures and Internet security practices
5. International cooperation at the level of governments, industry, consumer, business and anti-spam groups, to allow a global and coordinated approach to the problem.

In addition to the list above, during discussions and presentations the areas below were identified not in any order of priority as also important for cooperation and assistance to Member States, in which the ITU-D may be involved with entities with recognized expertise in the domain of Cybersecurity and combating spam:

¹ Paragraph c of “*Recognizing*” of WTDC06 Resolution 45 (Annex 1)

- a. Building basic awareness
- b. Appropriate national legislation
- c. Human and institutional capacity building
- d. Enforcement (capacity building domain)
- e. National policies and strategies on cybersecurity
- f. Exchange of information between countries and relevant stakeholders
- g. Establishment of national focal points
- h. Monitoring and evaluation of progress on existing initiatives
- i. Incident response, watch and warning.
- j. Assessment of cybersecurity vulnerabilities and threats.
- k. Effective tools and applications for network and cybersecurity
- l. Partnerships
- m. International cooperation

The meeting arrived at a consensus that ITU-D should play a key role in linking existing initiatives and provide a unifying framework bringing together these initiatives with the objective of addressing the needs of developing countries.

The meeting invited ITU-D to take account as appropriate of the relevant work of other stakeholders with recognized areas of expertise, such as ITU-T, London Action Plan, World Bank, Seoul-Melbourne Memorandum of Understanding (MoU), United Nations Office on Drugs and Crime, Council of Europe Convention on Cybercrime, Asia-Pacific Economic Cooperation Telecommunications and Information Working Group (APEC TEL), Organisation for Economic Co-operation and Development (OECD) anti-spam efforts and other relevant partners.

For the above-listed areas, the meeting recommended that the BDT under the coordination of Programme 3 should develop a project as the mechanism for the implementation of WTDC06 Resolution 45. Based on the needs and priorities of developing countries that request ITU assistance in this domain, the project should take account as appropriate, of recognised sources expertise and exiting initiatives including but not limited to: ITU-T, London Action Plan, World Bank, Seoul-Melbourne Memorandum of Understanding (MoU), United Nations Office on Drugs and Crime, Council of Europe Convention on Cybercrime, Asia-Pacific Economic Cooperation Telecommunications and Information Working Group (APEC TEL), Organisation for Economic Co-operation and Development (OECD) anti-spam efforts and other relevant partners.

Regarding the Project:

- Titled "Project for enhancing cooperation on Cybersecurity and combating spam", the project will have the duration of 4 years beginning from 2007 and be part of BDT Operational Plan for 2007.
- Annual reports will be made to ITU Council sessions on progress achieved in its implementation.
- The project in its implementation should take into account decisions of the WTDC06 on the mandate of the Development Sector in Cybersecurity and combating spam.
- The project should aim primarily at providing assistance to developing countries in the areas identified above by the meeting as vital for cooperation in the domain of Cybersecurity and combating spam.
- With regards to relevant legislation, take into account as appropriate, the relevant work of the Council of Europe when assisting countries in the development of national legislation in line with the Convention on Cybercrime
- Implementation of activities under the framework of this project should be based on expressed requests of countries with emphasis on developing countries.

- After the development of the project, it should be presented to potential funding entities including Member States, private sector and international organizations such as the World Bank and the European Commission.
-

**Annex 1****Resolution 45 (DOHA, 2006)****Mechanisms for enhancing cooperation on cybersecurity,
including combating spam**

The World Telecommunication Development Conference (Doha, 2006),

recalling

- a) the noble principles, aims and objectives embodied in the United Nations Charter and the Universal Declaration of Human Rights;
- b) its fundamental support for Programme 3 (e-strategies and ICT-applications), confirming that the latter shall have primary responsibility for Action Line C5 in the Tunis Agenda (Building confidence and security in the use of ICTs);
- c) the provisions of §§ 35, 36 and 37 of the Geneva Declaration of Principles;
- d) the provisions of § 15 of the Tunis Commitment,

considering

- a) the role of ICTs as effective tools to promote peace, security and stability and to enhance democracy, social cohesion, good governance and the rule of law, and the need to confront challenges and threats resulting from the abuse of this technology, including for criminal and terrorist purposes, while respecting human rights (§ 15 of the Tunis Commitment);
- b) the need to build confidence and security in the use of ICTs (§ 39 of the Tunis Agenda) and to prosecute cybercrime, at national and regional levels, noting existing frameworks, for example, Resolutions 55/63 and 56/121 of the General Assembly of the United Nations on "Combatting the criminal misuse of information technologies" and regional initiatives including, but not limited to, the Council of Europe's Convention on Cybercrime;
- c) that the considerable losses which ICT systems have incurred from the growing problem of cybercrime worldwide should alarm the entire international community, and ITU in particular;
- d) the need, through a multi-pronged approach, including international cooperation, to counter the problem associated with cybersecurity, including spam, which has not been given the necessary priority as called for in the Tunis Agenda (§ 41);
- e) the reasons behind the adoption of Resolution 37 (Istanbul, 2002) on bridging the digital divide, having regard to the action lines referenced in § 108 of the Tunis Agenda, including "Building confidence and security in the use of ICTs",

recalling

- a) desire and commitment of all concerned to build a people-centred, inclusive and development-oriented information society, premised on the purposes and principles of the Charter of the United Nations, international law and multilateralism, and respecting fully and upholding the Universal Declaration of Human Rights, so that people everywhere can create, access, utilize and share information and knowledge, to achieve their full potential and to attain the internationally agreed development goals and objectives, including the Millennium Development Goals;
- b) the provisions of §§ 4, 5 and 55 of the Geneva Declaration of Principles, and that freedom of expression and the free flow of information, ideas and knowledge are beneficial to development;
- c) that the Tunis Summit represented a unique opportunity to raise awareness of the benefits that ICTs can bring to humanity and the manner in which they can transform people's activities, interaction and lives, and thus increase confidence in the future,

recognizing

- a) the provisions for privacy and freedom of expression as contained in the relevant parts of the Universal Declaration of Human Rights (§ 42 of the Tunis Agenda);
- b) the need to safeguard the ethical dimensions of the information society in accordance with the Geneva Declaration of Principles and Action Plan (§ 43 of the Tunis Agenda), the need to counter terrorism (§ 44 of the Tunis Agenda) and the importance of continuity and stability of the internet (§ 45 of the Tunis Agenda), while ensuring respect for privacy and the protection of personal information and data (§ 46 of the Tunis Agenda);
- c) the need to effectively confront challenges and threats resulting from 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, and that it is necessary to work to prevent the abuse of information resources and technologies for criminal and terrorist purposes, while respecting human rights;
- d) the role of ICTs in the protection of children and in enhancing their development and that action to protect children from abuse and defend their rights in the context of ICTs should be strengthened, emphasizing that the best interests of the child are a key consideration,

noting

- a) that Resolution 50 (Florianópolis, 2004) of the World Telecommunication Standardization Assembly on cybersecurity is confined solely to the study of technical aspects for reducing the impact of this phenomenon;
- b) that spam is a significant and growing problem for users, networks and the internet as a whole, and spam and cybersecurity should be dealt with at appropriate national and international levels,

urges Member States

to provide the support necessary for implementation of this resolution,

resolves to instruct the Director of the Telecommunication Development Bureau

- 1 to organize, in conjunction with Programme 3 and based on member contributions, meetings of Member States and Sector Members to discuss ways to enhance cybersecurity including, *inter alia*, a memorandum of understanding to enhance cybersecurity and combat spam amongst interested Member States;
- 2 to report the results of these meetings to the 2006 plenipotentiary conference.
