RESOLUTION 130 (Rev. Guadalajara, 2010)

Strengthening the role of ITU in building confidence and security in the use of information and communication technologies

The Plenipotentiary Conference of the International Telecommunication Union (Guadalajara, 2010),

recalling

a) Resolution 130 (Rev. Antalya, 2006) of the Plenipotentiary Conference;

b) Resolution 69 (Hyderabad, 2010) of the World Telecommunication Development Conference (WTDC), on the creation of national computer incident response teams (CIRTs), particularly for developing countries, and cooperation between them;

c) that ITU Council Resolution 1305, adopted at its 2009 session, identified the security, safety, continuity, sustainability and robustness of the Internet as public policy issues that fall within the scope of ITU,

considering

a) the crucial importance of information and communication infrastructures and their applications to practically all forms of social and economic activity;

b) that, with the application and development of information and communication technologies (ICTs), new threats from various sources have emerged that have had an impact on confidence and security in the use of ICTs by all Member States, Sector Members and other stakeholders, including all users of ICTs, and on the preservation of peace and the economic and social development of all Member States, and that threats to and vulnerabilities of networks continue to give rise to ever-growing security challenges across national borders for all countries, in particular developing countries, including the least developed countries, small island developing states, landlocked developing countries and countries with economies in transition, while noting in this context the strengthening of ITU's role in building confidence and security in the use of ICTs and the need to further enhance international cooperation and develop appropriate existing national, regional and international mechanisms (for example, agreements, best practices, memorandums of understanding, etc);

c) that the ITU Secretary-General has been invited to support the International Multilateral Partnership Against Cyber-Threats (IMPACT), the Forum for Incident Response and Security Teams (FIRST) and other global or regional cybersecurity projects, as appropriate, and all countries, particularly developing countries, have been invited to take part in their activities;

d) the ITU Global Cybersecurity Agenda (GCA);

e) that, in order to protect these infrastructures and address these challenges and threats, coordinated national, regional and international action is required for prevention, preparation, response and recovery from computer security incidents, on the part of government

authorities, at the national (including the creation of national CIRTs), and sub-national levels, the private sector and citizens and users, in addition to international and regional cooperation and coordination, and that ITU has a lead role to play within its mandate and competencies in this field;

f) the need for continual evolution in new technologies to support the early detection of, and coordinated and timely response to, events or incidents compromising computer security, or computer network security incidents that could compromise the availability, integrity and confidentiality of critical infrastructures in ITU Member States, and for strategies that will minimize the impact of such incidents and mitigate the growing risks and threats to which such platforms are exposed*,*

recognizing

a) that the development of ICTs has been and continues to be instrumental for the growth and development of the global economy, underpinned by security and trust;

b) that the World Summit on the Information Society (WSIS) affirmed the importance of building confidence and security in the use of ICTs and the great importance of multistakeholder implementation at the international level, and established Action Line C5 (Building confidence and security in the use of ICTs), with ITU identified in the Tunis Agenda for the Information Society as moderator/facilitator for the action line, and that this task has been carried out by the Union in recent years, for example under GCA;

c) that WTDC-10 has adopted the Hyderabad Action Plan and its Programme 2, on cybersecurity and ICT applications and IP-based network related issues, which identifies cybersecurity as a priority activity of the Telecommunication Development Bureau (BDT) and defines activities to be undertaken by BDT; and has also adopted Resolution 45 (Hyderabad, 2010), on mechanisms for enhancing cooperation on cybersecurity, including countering and combating spam, calling on the Secretary-General to bring the resolution to the attention of the next plenipotentiary conference for consideration and required action, as appropriate; and Resolution 69 (Hyderabad, 2010), on the creation of national CIRTs, particularly for developing countries, and cooperation between them; and that moreover, a national IP-based public network security centre for developing countries is under study by Study Group 17 of the ITU Telecommunication Standardization Sector (ITU-T);

d) that, to support the creation of national CIRTs in Member States where these are needed and are currently absent, the World Telecommunication Standardization Assembly (WTSA) adopted Resolution 58 (Johannesburg, 2008), on encouraging the creation of national CIRTs, particularly for developing countries; and WTDC-10 adopted Resolution 69 (Hyderabad, 2010), on the creation of national CIRTs, particularly for developing countries, and cooperation between them;

e) § 15 of the Tunis Commitment, which states that: "*Recognizing the principles of universal and non-discriminatory access to ICTs for all nations, the need to take into account the level of social and economic development of each country, and respecting the development-oriented aspects of the information society, we underscore that ICTs are effective tools to promote peace, security and stability, to enhance democracy, social cohesion, good governance and the*

rule of law, at national, regional and international levels. ICTs can be used to promote economic growth and enterprise development. Infrastructure development, human capacity building, information security and network security are critical to achieve these goals. We further recognize 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. It is necessary to prevent the abuse of information resources and technologies for criminal and terrorist purposes, while respecting human rights", and that the challenges created by this misuse of ICT resources have only continued to increase since WSIS;

f) that Member States, in particular developing countries, in the elaboration of appropriate and workable legal measures relating to protection against cyberthreats at the national, regional and international levels, may require assistance from ITU in establishing technical and procedural measures, aimed at securing national ICT infrastructures, on request from these Member States, while noting that there are a number of regional and international initiatives which may support these countries in elaborating such legal measures;

g) Opinion 4 (Lisbon, 2009) of the World Telecommunication Policy Forum, on collaborative strategies for creating confidence and security in the use of ICTs;

h) the relevant outcomes of WTSA-08, notably:

i) Resolution 50 (Rev. Johannesburg, 2008), on cybersecurity;

ii) Resolution 52 (Rev. Johannesburg, 2008), on countering and combating spam;

i) that Resolution 69 (Hyderabad, 2010) provides for the establishment of CIRTs,

aware

a) that ITU and other international organizations, through a variety of activities, are examining issues related to building confidence and security in the use of ICTs, including stability and measures to combat spam, malware, etc., and to protect personal data and privacy;

b) that ITU-T Study Group 17, Study Groups 1 and 2 of the Telecommunication Development Sector (ITU-D) and other relevant ITU study groups continue to work on technical means for the security of information and communication networks, in accordance with Resolutions 50 and 52 (Rev. Johannesburg, 2008) and Resolutions 45 (Rev. Hyderabad, 2010) and 69 (Hyderabad, 2010);

c) that ITU has a fundamental role to play in building confidence and security in the use of ICTs;

d) that Opinion 4 (Lisbon, 2009), on collaborative strategies for creating confidence and security in the use of ICTs, invites ITU to pursue, principally on the basis of membership contributions and direction, further initiatives and activities, in close partnership with other concerned national, regional and international entities and organizations, consistent with Resolution 71 (Rev. Guadalajara, 2010) of this conference, on the strategic plan for the Union for 2012-2015, and all other relevant ITU resolutions;

e) that ITU-D Study Group 1 continues to carry out the studies called for in ITU-D Question 22-1/1 (Securing information and communications networks: best practices for developing a culture of cybersecurity), which has been reflected in United Nations General Assembly Resolution 64/211,

noting

a) that, as an intergovernmental organization with private-sector participation, ITU is well-positioned to play an important role, together with other relevant international bodies and organizations, in addressing threats and vulnerabilities, which affect efforts to build confidence and security in the use of ICTs;

b) §§ 35 and 36 of the Geneva Declaration of Principles and § 39 of the Tunis Agenda, on building confidence and security in the use of ICTs;

c) that although there are no universally agreed upon definitions of spam and other terms in this sphere, spam was characterized by ITU-T Study Group 2, at its June 2006 session, as a term commonly used to describe unsolicited electronic bulk communications over e-mail or mobile messaging (SMS, MMS), usually with the objective of marketing commercial products or services;

d) the Union's initiative concerning IMPACT and FIRST;

e) that BDT Programme 2 in the Hyderabad Action Plan was adopted with the understanding of the delegations to WTDC-10 that BDT does not draft laws,

bearing in mind

the work of the ITU established by Resolutions 50 and 52 (Rev. Johannesburg, 2008) and 58 (Johannesburg, 2008); Resolutions 45 (Rev. Hyderabad, 2010) and 69 (Hyderabad, 2010); BDT Programme 2 in the Hyderabad Action Plan; the relevant ITU-T Questions on technical aspects regarding the security of information and communication networks; and ITU-D Question 22-1/1,

resolves

1 to continue to give this work high priority within ITU, in accordance with its competences and expertise;

2 to give high priority to the work in ITU described under *bearing in mind* above, in accordance with its competences and areas of expertise, while being mindful of the need to avoid duplicating work among the Bureaux or the General Secretariat or work which more appropriately falls within the mandates of other intergovernmental and relevant international bodies;

3 that ITU shall focus resources and programmes on those areas of cybersecurity within its core mandate and expertise, notably the technical and development spheres, and not including areas related to Member States' application of legal or policy principles related to national defence, national security, content and cybercrime, which are within their sovereign rights, although this does not however exclude ITU from carrying out its mandate to develop technical

recommendations designed to reduce vulnerabilities in the ICT infrastructure, nor from providing all the assistance that was agreed upon at WTDC-10, including Programme 2 activities such as "*assisting Member States, in particular developing countries, in the elaboration of appropriate and workable legal measures relating to protection against cyberthreats*" and in activities under Question 22-1/1,

instructs the Secretary-General and the Directors of the Bureaux

1 to continue to review:

i) the work done so far in the three Sectors, under the ITU Global Cybersecurity Agenda initiative and in other relevant organizations, and initiatives to address existing and future threats in order to build confidence and security in the use of ICTs, such as the issue of countering spam, which is growing and on the rise;

ii) the progress achieved in the implementation of this resolution, with ITU continuing to play a lead facilitating role as the moderator/facilitator for Action Line C5, with the help of the advisory groups, consistent with the ITU Constitution and the ITU Convention;

2 consistent with Resolution 45 (Rev. Hyderabad, 2010) to work towards the preparation of a document relating to a possible memorandum of understanding (MoU), including the legal analysis of the MoU and its scope of application, among interested Member States, to strengthen cybersecurity and combat cyberthreats, in order to protect developing countries and any country interested in acceding to this possible MoU, with the outcome of the meeting to be submitted to the Council session in 2011 for its consideration and any action, as appropriate;

3 to facilitate access to tools and resources, within the available budget, required for enhancing confidence and security in the use of ICTs for all Member States, consistent with WSIS provisions on universal and non-discriminatory access to ICTs for all nations;

4 to continue to maintain the cybersecurity gateway as a way to share information on national, regional and international cybersecurity-related initiatives worldwide;

5 to report annually to the Council on these activities and to make proposals as appropriate;

6 to further enhance coordination between the study groups and programmes concerned,

instructs the Director of the Telecommunication Standardization Bureau

1 to intensify work within existing ITU-T study groups in order to:

i) address existing and future threats and vulnerabilities affecting efforts to build confidence and security in the use of ICTs, by developing reports or recommendations, as appropriate, with the goal of implementing the resolutions of WTSA-08, particularly Resolutions 50 and 52 (Rev. Johannesburg, 2008) and 58 (Johannesburg, 2008), allowing work to begin before a Question is approved;

ii) seek ways to enhance the exchange of technical information in these fields, promote the adoption of protocols and standards that enhance security, and promote international cooperation among appropriate entities;

iii) facilitate projects deriving from the outcomes of WTSA-08, in particular:

a) Resolution 50 (Rev. Johannesburg, 2008), on cybersecurity;

b) Resolution 52 (Rev. Johannesburg, 2008), on countering and combating spam;

2 to continue collaboration with relevant organizations with a view to exchanging best practices and disseminating information through, for example, joint workshops and training sessions and joint coordination activity groups, and, by invitation, through written contributions from relevant organizations,

instructs the Director of the Telecommunication Development Bureau

1 to develop, consistent with the results of WTDC-10 and pursuant to Resolution 45 (Rev. Hyderabad, 2010), Resolution 69 (Hyderabad, 2010) and Programme 2 in the Hyderabad Action Plan, the project for enhancing cooperation on cybersecurity and combating spam in response to the needs of developing countries, in close collaboration with the relevant partners;

2 upon request, to support ITU Member States in their efforts to build capacity, by facilitating Member States' access to resources developed by other relevant international organizations that are working on national legislation to combat cybercrime; supporting ITU Member States' national and regional efforts to build capacity to protect against cyberthreats/cybercrime, in collaboration with one another; consistent with the national legislation of Member States referred to above, assisting Member States, in particular developing countries, in the elaboration of appropriate and workable legal measures relating to protection against cyberthreats at national, regional and international levels; establishing technical and procedural measures, aimed at securing national ICT infrastructures, taking into the account the work of the relevant ITU-T study groups and, as appropriate, other relevant organizations; establishing organizational structures, such as CIRTs, to identify, manage and respond to cyberthreats, and cooperation mechanisms at the regional and international level;

3 to provide the necessary financial and administrative support for this project within existing resources, and to seek additional resources (in cash and in kind) for the implementation of this project through partnership agreements;

4 to ensure coordination of the work of this project within the context of ITU's overall activities in its role as moderator/facilitator for WSIS Action Line C5, and to eliminate any duplication regarding this important subject with the General Secretariat and ITU-T;

5 to coordinate the work of this project with that of the ITU-D study groups on this topic, and with the relevant programme activities and the General Secretariat;

6 to continue collaboration with relevant organizations with a view to exchanging best practices and disseminating information through, for example, joint workshops and training sessions;

7 to report annually to the Council on these activities and make proposals as appropriate,

further instructs the Director of the Telecommunication Standardization Bureau and the Director of the Telecommunication Development Bureau

each within the scope of his responsibilities:

1 to implement relevant resolutions of both WTSA-08 and WTDC-10, including Programme 2 on providing support and assistance to developing countries in building confidence and security in the use of ICTs;

2 to identify and promote the availability of information on building confidence and security in the use of ICTs, specifically related to the ICT infrastructure, for Member States, Sector Members and relevant organizations;

3 without duplicating the work under ITU-D Question 22-1/1, to identify best practices in establishing CIRTs, to prepare a reference guide for the Member States and, where appropriate, to contribute to Question 22-1/1;

4 to cooperate with relevant organizations and other relevant international and national experts, as appropriate, in order to identify best practices in the establishment of CIRTs;

5 to take action with a view to new Questions being examined by the study groups within the Sectors on the establishment of confidence and security in the use of ICT;

6 to support strategy, organization, awareness-raising, cooperation, evaluation and skills development;

7 to provide the necessary technical and financial support, within the constraints of existing budgetary resources, in accordance with Resolution 58 (Johannesburg, 2008);

8 to mobilize appropriate extrabudgetary resources, outside the regular budget of the Union, for the implementation of this resolution, to help developing countries,

instructs the Secretary-General

pursuant to his initiative on this matter:

1 to propose to the Council, taking into account the activities of the three Sectors in this regard, an action plan to strengthen the role of ITU in building confidence and security in the use of ICTs;

2 to cooperate with relevant international organizations, including through the adoption of MoUs, subject to the approval of the Council in this regard, in accordance with Resolution 100 (Minneapolis, 1998) of the Plenipotentiary Conference,

requests the Council

to include the report of the Secretary-General in the documents sent to Member States in accordance with No. 81 of the Convention,

invites Member States

to consider joining appropriate competent international and regional initiatives for enhancing national legislative frameworks relevant to the security of information and communication network,

invites Member States, Sector Members and Associates

1 to contribute on this subject to the relevant ITU study groups and to any other activities for which the Union is responsible;

2 to contribute to building confidence and security in the use of ICTs at the national, regional and international levels, by undertaking activities as outlined in § 12 of the Geneva Plan of Action, and to contribute to the preparation of studies in these areas;

3 to promote the development of educational and training programmes to enhance user awareness of risks in cyberspace.