RESOLUTION 45 (Rev. Dubai, 2014)

Mechanisms for enhancing cooperation on cybersecurity, including countering and combating spam

The World Telecommunication Development Conference (Dubai, 2014),

recalling

a) Resolution 130 (Rev. Guadalajara, 2010) of the Plenipotentiary Conference, on the role of ITU in building confidence and security in the use of information and communication technologies (ICTs);

b) Resolution 174 (Guadalajara, 2010) of the Plenipotentiary Conference, on ITU's role with regard to international public policy issues relating to the risk of illicit use of ICTs;

c) Resolution 179 (Guadalajara, 2010) of the Plenipotentiary Conference, on ITU's role in child online protection;

d) Resolution 181 (Guadalajara, 2010) of the Plenipotentiary Conference, on definitions and terminology relating to building confidence and security in the use of ICTs;

e) Resolution 45 (Rev. Hyderabad, 2010) of the World Telecommunication Development Conference (WTDC);

f) Resolution 50 (Rev. Dubai, 2012) of the World Telecommunication Standardization Assembly (WTSA), on cybersecurity;

g) Resolution 52 (Rev. Dubai, 2012) of WTSA, on countering and combating spam;

h) Resolution 58 (Rev. Dubai, 2012) of WTSA, on encouraging the creation of national computer incident response teams (CIRTs), particularly in developing countries;

i) Resolution 69 (Rev. Dubai, 2014) of this conference, on the creation of CIRTs, particularly for developing countries, and cooperation among them;

j) Resolution 67 (Rev. Dubai, 2014) of this conference, on the role of the ITU Telecommunication Development Sector (ITU-D) in child online protection;

k) the noble principles, aims and objectives embodied in the Charter of the United Nations and the Universal Declaration of Human Rights;

l) that ITU is the lead facilitator for Action Line C5 in the Tunis Agenda for the Information Society (Building confidence and security in the use of ICTs);

m) the cybersecurity-related provisions of the Tunis Commitment and the Tunis Agenda;

n) the goal set out in the strategic plan for the Union for 2012-2015, approved by Resolution 71 (Rev. Guadalajara, 2010) of the Plenipotentiary Conference, which calls on ITU-D to promote the availability of infrastructure and foster an enabling environment for telecommunication/ICT infrastructure development and its use in a safe and secure manner;

o) Question 22 of ITU-D Study Group 1, under which in the previous cycle many members collaborated to produce reports, including course materials for use in developing countries, such as a compendium of national experiences, best practices for public-private partnerships, best practices for building a CIRT with accompanying course material, and best practices for a CIRT management framework;

p) the report of the Chairman of the High-Level Group of Experts (HLEG) of the Global Cybersecurity Agenda (GCA), established by the ITU Secretary-General pursuant to the requirements of Action Line C5 on building confidence and security in the use of ICTs and in accordance with Resolution 140 (Rev. Guadalajara, 2010) of the Plenipotentiary Conference, on the role of ITU as sole facilitator for World Summit on the Information Society (WSIS) Action Line C5, and Resolution 58 (Rev. Dubai, 2012), on encouraging the creation of national CIRTs, particularly for developing countries;

q) that ITU and the United Nations Office on Drugs and Crime (UNODC) have signed a memorandum of understanding (MoU) in order to strengthen security in the use of ICTs,

considering

a) the role of telecommunications/ICTs as effective tools to promote peace, economic development, security and stability and to enhance democracy, social cohesion, good governance and the rule of law, and the need to confront the escalating challenges and threats resulting from the abuse of this technology, including for criminal and terrorist purposes, while respecting human rights (see also § 15 of the Tunis Commitment);

b) the need to build confidence and security in the use of telecommunications/ICTs by strengthening the trust framework (§ 39 of the Tunis Agenda), and the need for governments, in cooperation with other stakeholders within their respective roles, to develop necessary legislation for the investigation and prosecution of cybercrime at national levels, and cooperate at regional and international levels having regard to existing frameworks;

c) that United Nations General Assembly (UNGA) Resolution 64/211 invites Member States to use, if and when they deem appropriate, the voluntary self-assessment tool that is annexed to the resolution for national efforts;

d) the need for Member States to develop national cybersecurity programmes centred around a national plan, public-private partnerships, a sound legal foundation, an incident management, watch, warning, response and recovery capability, and a culture of awareness, using as a guide the reports on best practices for a national approach to cybersecurity: building blocks for organizing national cybersecurity efforts, drawn up under the two study periods of Question 22 of ITU-D Study Group 1;

e) that the considerable and increasing losses which users of telecommunication/ICT systems have incurred from the growing problem of cybercrime and deliberate sabotage worldwide alarm all developed and developing nations of the world without exception;

f) the reasons behind the adoption of Resolution 37 (Rev. Dubai, 2014) of this conference, on bridging the digital divide, having regard to the importance of multistakeholder implementation at the international level and to the action lines referenced in § 108 of the Tunis Agenda, including "Building confidence and security in the use of ICTs";

g) the outcomes of several ITU activities related to cybersecurity, especially, but not limited to, the ones coordinated by the Telecommunication Development Bureau, in order to fulfil ITU's mandate as facilitator for the implementation of Action Line C5 (Building confidence and security in the use of ICTs);

h) that various organizations from all sectors of society work in collaboration to enhance cybersecurity of telecommunications/ICTs;

i) that Objective 3 of ITU-D, set under the strategic plan for the Union for 2012-2015, contained in Resolution 71 (Rev. Guadalajara, 2010), was to foster the development of strategies to enhance the deployment, and the safe, secure and affordable use of ICT applications and services towards mainstreaming telecommunications/ICTs in the broader economy and society;

j) that the fact, among others, that critical telecommunication/ICT infrastructures are interconnected at global level means that low infrastructure security in one country could result in greater vulnerability and risks in others;

k) that various information, materials, best practices and financial resources, as appropriate, are available to Member States from national, regional and other relevant international organizations, according to their respective roles;

l) that the results of the cybersecurity awareness survey conducted by BDT and Question 22-1/1 in the previous study period showed that least developed countries require substantial assistance in this area;

m) that the ITU Global Cybersecurity Agenda (GCA) encourages international cooperation aimed at proposing strategies for solutions to enhance confidence and security in the use of telecommunications/ICTs,

recognizing

a) that measures undertaken to ensure the stability and security of telecommunication/ICT networks, to protect against cyberthreats/cybercrime and to counter spam must protect and respect the provisions for privacy and freedom of expression as contained in the relevant parts of the Universal Declaration of Human Rights (see also § 42 of the Tunis Agenda) and the International Covenant on Civil and Political Rights;

b) that UNGA Resolution 68/167, on the right to privacy in the digital age, affirms, *inter alia*, "that the same rights the people have off line must also be protected on line, including the right to privacy";

c) the need to take appropriate actions and preventive measures, as determined by law, against abusive uses of telecommunications/ICTs, as mentioned in connection with "Ethical dimensions of the information society" in the Geneva Declaration of Principles and Plan of Action (§ 43 of the Tunis Agenda), the need to counter terrorism in all its forms and manifestations on telecommunication/ICT networks, while respecting human rights and complying with other obligations under international law, as outlined in operative paragraph 81 of UNGA Resolution 60/1 on the 2005 world summit outcome, the importance of the security, continuity and stability of telecommunication/ICT networks and the need to protect telecommunication/ICT networks from threats and vulnerabilities (§ 45 of the Tunis Agenda), while ensuring 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 (§ 46 of the Tunis Agenda);

d) the need to effectively confront challenges and threats resulting from the use of telecommunications/ICTs such as 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 to work cooperatively to prevent the abuse of information resources and technologies for criminal and terrorist purposes, while respecting human rights;

e) the role of telecommunications/ICTs in the protection of children and in enhancing their development, and the need to strengthen action to protect children and youth from abuse and defend their rights in the context of telecommunications/ICTs, emphasizing that the best interests of the child are a key consideration;

f) the desire and commitment of all concerned to build a people-centred, inclusive and secure 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 in complete security, in order to achieve their full potential and to attain the internationally agreed development goals and objectives, including the Millennium Development Goals;

g) 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;

h) that the Tunis phase of WSIS represented a unique opportunity to raise awareness of the benefits that telecommunications/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, conditional upon the secure use of telecommunications/ICTs, as the implementation of the Summit outcomes has demonstrated;

i) the need to deal effectively with the significant problem posed by spam, as called for in § 41 of the Tunis Agenda, as well as, *inter alia*, spam, cybercrime, viruses, worms and denial-of-service attacks;

j) the need for effective coordination between ITU-D programmes and Questions,

noting

a) the continuing work of Study Group 17 (security) of the ITU Telecommunication Standardization Sector (ITU-T) and other standards-development organizations on various aspects of security of telecommunications/ICT;

b) that spam is a significant problem and continues to pose a threat for users, networks and the Internet as a whole, and that the issue of cybersecurity should be addressed at appropriate national, regional and international levels;

c) that cooperation and collaboration among Member States, Sector Members and relevant stakeholders contributes to building and maintaining a culture of cybersecurity,

resolves

1 to continue to recognize cybersecurity as one of ITU's priority activities and to continue to address, within its area of core competence, the issue of securing and building confidence in the use of telecommunications/ICTs, by raising awareness, identifying best practices and developing appropriate training material in order to promote a culture of cybersecurity;

2 to enhance collaboration and cooperation with, and share information among, all relevant international and regional organizations on cybersecurity-related initiatives within ITU's areas of competence, taking into account the need to assist developing countries,

instructs the Director of the Telecommunication Development Bureau

1 to continue to organize, in collaboration with relevant organizations, as appropriate, in conjunction with the programme under Output 3.1 of Objective 3, based on member contributions, and in cooperation with the Director of the Telecommunication Standardization Bureau (TSB), meetings of Member States, Sector Members and other relevant stakeholders to discuss ways and means to enhance cybersecurity;

2 to continue, in collaboration with relevant organizations and stakeholders, to carry out studies on strengthening the cybersecurity of developing countries at regional and international level, based on a clear identification of their needs, particularly those relating to telecommunication/ICT use, including the protection of children and youth;

3 to support Member States' initiatives, especially in developing countries, regarding mechanisms for enhancing cooperation on cybersecurity;

4 to assist the developing countries in enhancing their states of preparedness in order to ensure a high and effective level of security for their critical telecommunication/ICT infrastructures;

5 to assist Member States in the establishment of an appropriate framework between developing countries allowing rapid response to major incidents, and propose an action plan to increase their protection, taking into account mechanisms and partnerships, as appropriate;

6 to implement this resolution in cooperation and collaboration with the Director of TSB;

7 to report the results of the implementation of this resolution to the next WTDC,

invites the Secretary-General, in coordination with the Directors of the Radiocommunication Bureau, the Telecommunication Standardization Bureau and the Telecommunication Development Bureau

1 to report on MoUs between countries, as well as existing forms of cooperation, providing analysis of their status, scope and applications of these cooperative mechanisms to strengthen cybersecurity and combat cyberthreats, with a view to enabling Member States to identify whether additional memoranda or mechanisms are required;

2 to support regional and global cybersecurity projects, such as IMPACT, FIRST, OAS, APCERT, among others, and to invite all countries, particularly developing ones, to take part in these activities,

requests the Secretary-General

1 to bring this Resolution to the attention of the next plenipotentiary conference for consideration and required action, as appropriate;

2 to report the results of these activities to the Council and to the Plenipotentiary Conference in 2018,

invites Member States, Sector Members, Associates and Academia

1 to provide the necessary support for and participate actively in the implementation of this resolution;

2 to recognize cybersecurity and countering and combating spam as high-priority items, and to take appropriate action and contribute to building confidence and security in the use of telecommunications/ICTs at the national, regional and international level;

3 to encourage service providers to protect themselves from the risks identified, endeavour to ensure the continuity of services provided and notify security infringements,

invites Member States

1 to establish an appropriate framework allowing rapid response to major incidents, and propose an action plan to prevent and mitigate such incidents;

2 to establish strategies and capabilities at the national level to ensure protection of national critical infrastructures, including enhancing the resilience of telecommunication/ICT infrastructures.