RESOLUTION 45 (REV. HYDERABAD, 2010)

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

The World Telecommunication Development Conference (Sharm El Sheik, 2014),

recalling

a) Resolution 45 (Doha, 2006) of the World Telecommunication Development Conference (WTDC);

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

c) its fundamental support for Programme 3 (e-strategies and ICT-applications), confirming that ITU shall play a leading facilitating role for Action Line C5 in the Tunis Agenda for the Information Society (Building confidence and security in the use of ICTs);

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

e) Goal 4 of the strategic plan for the Union for 2008-2011, approved by Resolution 71 (Rev. Antalya, 2006) of the Plenipotentiary Conference, which states that ITU can achieve its overall mission by developing tools, based on contributions from the membership, to promote end-user confidence, and to safeguard the efficiency, security, integrity and interoperability of networks;

f) Resolution 130 (Antalya, 2006) of the Plenipotentiary Conference, which resolves to give high priority to the role of ITU in building confidence and security in the use of telecommunications/information and communication technologies (ICTs);

g) the adoption at WTDC (Doha, 2006) of a new Question 22/1, entitled "Securing information and communication networks: best practices for developing a culture of cybersecurity";

h) 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 (Antalya, 2006) of the Plenipotentiary Conference, on the role of ITU as sole facilitator for WSIS Action Line C5, and Resolution 58 (Johannesburg, 2008) of the World Telecommunication Standardization Assembly (WTSA), on encouraging the creation of national computer incident response teams, particularly for developing countries;

i) Resolution [COM 3/9] of this conference, on the creation of national and regional computer incident response teams, particularly for developing countries, and cooperation among them,

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 the escalating challenges and growing 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, regional and international levels, having regard to existing frameworks, for example: United Nations General Assembly (UNGA) Resolutions 55/63 and 56/121 on combating the criminal misuse of information technologies and Resolutions 57/239, 58/199 and 64/211 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures; regional initiatives including, but not limited to, the Council of Europe's Convention on Cybercrime (§ 40 of the Tunis Agenda); and international partnerships;

c) that 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, a watch, warning, response and recovery capability, and a culture of awareness, using as a guide the Report on best practices for a national approach to cybersecurity: building blocks for organizing national cybersecurity efforts, drawn up under Question 22 of Study Group 1 of the ITU Telecommunication Development Sector (ITU-D);

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. Hyderabad, 2010) 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 Objective 1 of ITU-D, set under the strategic plan for the Union for 2008-2011, approved in Resolution 71 (Rev. Antalya, 2006), is to organize and strengthen cooperation among ITU-D members and between ITU-D and other stakeholders, reflecting the relevant WSIS outcomes;

i) 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,

recalling further

a) the 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, in order 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 the fact that freedom of expression and the free flow of information, ideas and knowledge are beneficial to development;

c) 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,

recognizing

a) that measures undertaken to ensure the stability and security of ICT networks, to fight 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);

b) the need to take appropriate actions and preventive measures, as determined by law, against abusive uses of 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 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 ICT networks and the need to protect 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);

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

d) 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;

e) 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;

f) the provisions of §§ 4, 5 and 55 of the Geneva Declaration of Principles, and the fact that freedom of expression and the free flow of information, ideas and knowledge are beneficial to development;

g) that the Internet supports the free flow of information, ideas and knowledge in part through its foundational support for innovative and flexible modes of interaction with and collaborative use of information offered to the public online, and policies to address security-related issues that may relate to information products may have general effects on this flexibility if it is not considered carefully in the development of security-related issues;

~~g~~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;

~~h~~i) the need to deal effectively with the significant and growing 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, as called for in Goal 4 of the strategic plan in Annex 1 to Resolution 71 (Rev. Antalya, 2006),

noting

a) that Resolution 50 (Johannesburg, 2008) of WTSA, on cybersecurity, and Resolution 52 (Johannesburg, 2008) of WTSA, on countering and combating spam, include the study of technical aspects for reducing the impact of these phenomena;

b) the work of Study Group 17 (security) of the ITU Telecommunication Standardization Sector (ITU-T) on public key infrastructures, identity management, digital signatures, the security manual, the security standards roadmap and the cybersecurity information exchange framework;

c) that cryptographic measures such as those referenced above as undergoing study in relation to security by ITU-T Study Group 17 may be utilized in support of security-related policy and proposals may arise to implement them as components of technological infrastructure in ways that may extend their effects more broadly than their intended purposes to serve security-related concerns, potentially impacting the free flow of information, ideas and knowledge and the flexible modes of interaction with and collaborative use of information available online that the Internet makes possible, or potentially impacting issues related to Internet resources such as domain names and IP addresses;

~~e~~d) that the enormous increase in spam is a significant and growing problem 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, with the aim of combating spam, in particular criminal spam;

~~d~~e) 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 ICTs;

~~e~~f) that cooperation and collaboration among Sector Members contributes to building and maintaining a culture of cybersecurity,

resolves

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

2 to incorporate recognition of the flexible foundation provided by the Internet and its support for flexible modes of interactive and collaborative uses of information offered online while addressing the issue of securing and building confidence in ICTs as described above, noting that policies in this area could have broader unforeseen effects otherwise, including effects on the free flow of information, ideas and knowledge, or effects on issues related to Internet resources such as domain names and IP addresses, if this consideration is not incorporated distinctly; and noting this concern particularly in relation to the use of cryptographic measures such as digital signatures;

~~2~~3 to continue to collaborate, cooperate and share information among relevant international and regional organizations on cybersecurity-related initiatives within its areas of competence,

instructs the Director of the Telecommunication Development Bureau

1 to continue to organize, in conjunction with Programme 2 and based on member contributions, and in collaboration with the Director of the Telecommunication Standardization Bureau, meetings of Member States, Sector Members and other appropriate relevant stakeholders to discuss ways and means to enhance cybersecurity;

2 to carry out studies on strengthening the cybersecurity of developing countries at regional and universal 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 assure that careful consideration of potential impacts that security-related measures may have on the free flow of information, ideas and knowledge, on the flexible foundation provided by the Internet and its support for flexible modes of interactive and collaborative uses of information online, or on issues related to Internet resources such as domain names and IP addresses, as referenced under "recognizing," "noting" and "resolves" above, is incorporated in activities undertaken to enhance online security, noting this concern particularly in relation to the use of cryptographic technological means to support security-related policy;

~~3~~4 to support Member States' initiatives regarding mechanisms for enhancing cooperation on cybersecurity;

~~4~~5 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~~6 to assist Member States in the establishment of an appropriate framework between the developing countries allowing rapid response to major incidents, and propose an action plan to increase their protection;

~~6~~7 to continue to cooperate with the Secretary-General's initiative on cybersecurity, and with the other ITU Sectors in accordance with the Bureau's mandate;

~~7~~8 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 work towards the preparation of a document relating to a possible memorandum of understanding (MoU) among interested Member States, including the legal analysis of the MoU and its scope of application, 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 at its 2011 session for consideration and any action, as appropriate;

2 to support IMPACT, FIRST and other global or regional cybersecurity projects, as appropriate, and to invite all countries, particularly developing countries, to take part in its 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 2014,

invites Member States and Sector Members

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

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

3 to encourage access providers to protect themselves from the risks identified, guarantee the continuity of services provided and notify security infringements,

invites Member States

to establish an appropriate framework allowing rapid response to major incidents, and propose an action plan to increase their protection.