INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

WORLD TELECOMMUNICATION STANDARDIZATION ASSEMBLY
Dubai, 20-29 November 2012

Resolution 50 – Cybersecurity

CAUTION !

PREPUBLISHED RESOLUTION

This prepublication is an unedited version of a recently approved Resolution. It will be replaced by the published version after editing. Therefore, there will be differences between this prepublication and the published version.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

RESOLUTION 50

Cybersecurity

(Florianópolis, 2004; Johannesburg, 2008; Dubai, 2012)

The World Telecommunication Standardization Assembly (Dubai, 2012),

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;

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 information and communication technologies;

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 information and communication technologies;

e) Resolutions 55/63 and 56/121 of the United Nations General Assembly, which established the legal framework on countering the criminal misuse of information technologies;

f) Resolution 57/239 of the United Nations General Assembly, on the creation of a global culture of cybersecurity;

g) Resolution 58/199 of the United Nations General Assembly, on the creation of a global culture of cybersecurity and the protection of essential information infrastructures;

h) Resolution 41/65 of the United Nations General Assembly, on principles relating to remote sensing of the Earth from outer space;

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

j) Resolution 52 (Rev. Johannesburg, 2008) of the World Telecommunication Standardization Assembly (WTSA), on countering and combating spam;

k) Resolution 58 (Johannesburg, 2008) of WTSA, on encouraging the creation of national computer incidence response teams, particularly in developing countries[1],

considering

a) the crucial importance of the information and communication technologies (ICT) infrastructure to practically all forms of social and economic activity;

b) that the legacy public switched telephone network (PSTN) has a level of inherent security properties because of its hierarchical structure and built-in management systems;

---

[1] These include the least developed countries, small island developing states, landlocked developing countries and countries with economies in transition.

c) that IP networks provide reduced separation between user components and network components if adequate care is not taken in the security design and management;

d) that the converged legacy networks and IP networks are therefore potentially more vulnerable to intrusion if adequate care is not taken in the security design and management of such networks;

e) that there are cyberincidents caused by cyberattacks, for example malicious or thrill-seeker intrusions using malware (such as worms and viruses), distributed by various methods, for example distribution by web and bot-infected computers;

f) that in order to protect global telecommunication/ICT infrastructures from the threats and challenges of the evolving cybersecurity landscape, coordinated national, regional and international action is required to protect from and respond to various forms of impairing events;

g) that the ITU Telecommunication Standardization Sector (ITU-T) has a role to play within its mandate and competencies in *considering f)*,

considering further

a) that Recommendation ITU-T X.1205 provides a definition, a description of technologies, and network protection principles;

b) that Recommendation ITU-T X.805 provides a systematic framework for identifying security vulnerabilities, and Recommendation ITU-T X.1500 provides the cybersecurity information exchange (CYBEX) model and discusses techniques that could be used to facilitate the exchange of cybersecurity information;

c) that ITU-T and the Joint Technical Committee for Information Technology (JTC 1) of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) already have a significant body of published materials and ongoing work that is directly relevant to this topic, which needs to be considered,

recognizing

a) the relevant outcomes of the World Summit on the Information Society (WSIS) identified ITU as the facilitator and moderator for Action Line C5 (Building confidence and security in the use of ICTs);

b) the *resolves* paragraph of Resolution 130 (Rev. Guadalajara, 2010) of the Plenipotentiary Conference, on strengthening the role of ITU in building confidence and security in the use of information and communication technologies, and the instruction to intensify work with high priority within the ITU-T study groups;

c) that Programme 2, on cybersecurity, ICT applications and IP-based network related issues adopted by WTDC (Hyderabad, 2010) includes cybersecurity as one of its priority activities and relevant activities to be undertaken by BDT, and that Question 22/1 of the ITU Telecommunication Development Sector (ITU-D) addresses the issue of securing information and communication networks through the identification of best practices for developing a culture of cybersecurity, and Resolution 45 (Rev. Hyderabad, 2010 of WTDC), on mechanisms for enhancing cooperation on cybersecurity, including countering and combating spam, was adopted;

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

recognizing further

a) that cyberattacks such as phishing, pharming, scan/intrusion, distributed denials of service, web-defacements, unauthorized access, etc., are emerging and having serious impacts;

b) that botnets are used to distribute bot-malware and carry out cyberattacks;

c) that sources of attacks are sometimes difficult to identify (for example, attacks using spoofed IP addresses);

d) that cybersecurity is one of the elements for building confidence and security in the use of telecommunications/ICTs;

e) that, in accordance with Resolution 181 (Guadalajara, 2010), it is recognized that it is important to study the issue of terminology related to building confidence and security in the use of ICTs, that this base set needs to include other important issues in addition to cybersecurity and that the definition of cybersecurity may need to be modified from time to time to reflect changes in policy;

f) that Resolution 181 (Guadalajara, 2010), resolved to take into account the definition of the term cybersecurity approved in Recommendation ITU-T X.1205 for use in ITU activities related to building confidence and security in the use of ICTs;

g) that, as recognized in Resolution 181 (Guadalajara, 2010), ITU-T Study Group 17 is responsible for developing the core Recommendations on telecommunication and ICT security,

noting

a) the vigorous activity and interest in the development of telecommunication/ICT security standards and Recommendations in ITU-T Study Group 17, the lead ITU-T study group on security, and in other standardization bodies, including the Global Standards Collaboration (GSC) group;

b) that there is a need for national, regional and international strategies and initiatives to be harmonized to the extent possible, in order to avoid duplication and to optimize the use of resources;

c) that cooperation and collaboration among organizations addressing security issues can promote progress and contribute to building and maintaining a culture of cybersecurity;

d) that, as recognized in Resolution 130 (Rev. Guadalajara, 2010), a national IP-based public network security centre for developing countries is under study by ITU-T Study Group 17, and some work has been completed in this area, including the ITU-T X.800- ITU-T X.849 series of Recommendations and its Supplements,

resolves

1 that all ITU-T study groups continue to evaluate existing and evolving new Recommendations, and especially signalling and telecommunication protocol Recommendations, with respect to their robustness of design and potential for exploitation by malicious parties to interfere destructively with their deployment in the global information and telecommunication infrastructure, develop new Recommendations for emerging security issues and take into account new services and applications to be supported by the global telecommunication/ICT infrastructure (e.g. cloud computing, smart grid and intelligent transport systems, which are based on telecommunication/ICT networks);

2 that ITU-T continue to raise awareness, within its area of operation and influence, of the need to defend information and telecommunication systems against the threat of cyberattack, and continue to promote cooperation among appropriate international and regional organizations in

order to enhance exchange of technical information in the field of information and telecommunication network security;

3 that ITU-T should work closely with ITU-D, particularly in the context of Question 22/1;

4 that, in assessing networks and protocols for security vulnerabilities and facilitation of exchanging cybersecurity information, ITU-T Recommendations, including the ITU-T X-series of Recommendations and their Supplements, among them ITU-T X.805, ITU-T X.1205, ITU-T X.1500, ISO/IEC standards and other relevant deliverables from other organizations, be taken into consideration and applied as appropriate;

5 that ITU-T continue work on the development and improvement of terms and definitions related to building confidence and security in the use of telecommunications/ICTs, including the term cybersecurity;

6 that concerned parties are invited to work together to develop standards and guidelines in order to protect against cyberattacks, and facilitate tracing the source of an attack;

7 that global, consistent and interoperable processes for sharing incident-response related information should be promoted;

8 that all ITU-T study groups continue to provide regular reports on security of telecommunications/ICT to the Telecommunication Standardization Advisory Group (TSAG) on progress in evaluating existing and evolving new Recommendations;

9 that ITU-T study groups continue to liaise with standards development organizations and other bodies active in this field, such as ISO/IEC JTC1, the Organisation for Economic Co-operation and Development (OECD), the Asia-Pacific Economic Cooperation Telecommunication and Information Working Group (APEC-TEL) and the Internet Engineering Task Force (IETF);

10 that ITU-T Study Group 17 continue its work on the issues raised in Resolution 130 (Rev. Guadalajara, 2010), and on the ITU-T X-series of Recommendations, including Supplements as appropriate,

instructs the Director of the Telecommunication Standardization Bureau

1 to prepare, in building upon the information base associated with the *ICT Security Standards Roadmap* and the ITU-D efforts on cybersecurity, and with the assistance of other relevant organizations, an inventory of national, regional and international initiatives and activities to promote, to the maximum extent possible, the worldwide harmonization of strategies and approaches in this critically important area;

2 to report annually to the ITU Council, as specified in Resolution 130 (Guadalajara, 2010), on progress achieved in the actions outlined above;

3 to continue to recognize the role played by other organizations with experience and expertise in the area of security standards, and coordinate with those organizations as appropriate,

further instructs the Director of the Telecommunication Standardization Bureau

1 to continue to follow up WSIS activities on building confidence and security in the use of ICTs, in cooperation with relevant stakeholders, as a way to share information on national, regional and international and non-discriminatory cybersecurity-related initiatives globally;

2 to cooperate with the BDT in relation to any item concerning cybersecurity in accordance with Resolution 45 (Rev. Hyderabad, 2010),

3 to continue to cooperate with the Secretary-General's Global Cybersecurity Agenda (CGA) and with IMPACT, FIRST and other global or regional cybersecurity projects, as appropriate, to develop relationships and partnerships with various regional and international cybersecurity-related organizations and initiatives, as appropriate, and to invite all Member States, particularly developing countries, to take part in these activities and to coordinate and cooperate with these different activities;

4 taking into account Resolution 130 (Rev. Guadalajara 2010), to work collaboratively with the other Directors of the Bureaux to support the Secretary-General in preparing a document relating to a possible memorandum of understanding (MoU) (according to Resolution 45 (Rev. Hyderabad, 2010)) 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,

invites Member States, Sector Members, Associates and academia, as appropriate

to cooperate and participate actively in the implementation of this resolution and the associated actions.