|  |  |  |
| --- | --- | --- |
| itu_logo | World Telecommunication Standardization Assembly (WTSA-16)Hammamet, 25 October - 3 November 2016 | CCITT/ITU-T 60th Anniversary logo |
|  |  |
|  |  |
| PLENARY MEETING | Addendum 19 toDocument 46-E |
|  | 22 September 2016 |
|  | Original: English |
|  |
| Member States of the Inter-American Telecommunication Commission (CITEL) |
| Proposed modification to WTSA-12 Resolution 50 - Cybersecurity |
|  |
|  |

|  |  |
| --- | --- |
| **Abstract:** | This contribution proposes edits to Resolution 50 (Rev. Dubai, 2012) to update the text in line with Resolution 130 (Rev. Busan, 2014) and Resolution 45 (Rev. Dubai, 2014). These revisions will help ensure that the resolution reflects the current global state of play in the area of building confidence and security in the use of ICTs and that the ITU-T’s contribution on this topic is in alignment with Membership’s agreed goals and priorities. |

Introduction

Information and communication technologies (ICTs) are integral to economic and social development. Security is an essential element of the operation and use of ICTs and requires that all persons involved be aware of security and take action appropriate to their role. As the use of ICT continues to grow, cybersecurity continues to be a priority among ITU Membership. Over the last four years, the ITU-T’s Study Group 17 continued its work in this area as did many other standards development organizations and consortia at the national, regional, and international levels. In addition, the 2014 ITU Plenipotentiary Conference and the 2014 World Telecommunication Development Conference agreed to goals and priorities in the area of building confidence and security in the use of ICTs to which the ITU-T is expected to contribute. CITEL therefore believes it is relevant to update Resolution 50 to ensure it is in line with these developments.

Cybersecurity has earned itself a place of concern for experts – ITU among them, users and, mainly States.

Since the last Assembly until now, Cybersecurity issues have not only maintained, but also increased their importance in terms of requiring attention and involvement of the Information and Communication Technologies Sector. For this reason, the present Resolution, its terms and relevance are maintained as an essential element as regards standardization and as a prominent instrument of the Union and its members.

In this proposal for modification, the Argentine Republic believes that the terms of the Resolution must be kept, and in turn proposes its updating in order to incorporate the new cybersecurity-related elements arising from the trends in certain emerging areas and mainly from new threats. Also, we propose to incorporate those elements coming from the last World Telecommunication Development Conference (WTDC-14), the one that approved the contribution of ITU-D to the Strategic Plan of ITU for 2016-2019, endorsing five Objectives, among these Objective 3 – Enhance confidence and security in the use of telecommunications/ICTs, as well as enhanced deployment of ICT applications and services; and Outcome 3.1 of said Objective: Improved confidence and security in the use of ICTs and services, within whose execution framework is the Cybersecurity Programme.

Among the elements and new emerging areas, we can mention the increased value that users and/or devices have for attackers as the degree of physical interconnection and exchange of information grows, giving rise to new uses such as, e-banking, affidavits and mainly smart phone applications.

Likewise, the current advance and development of the Internet of Things create a broad scope outlook in terms of devices and activities and, at the same time, in terms of threats.

Proposal

CITEL proposes revisions to Resolution 50 (Rev. Dubai 2012) to update updated the text in line with Resolution 130 (Rev. Busan, 2014) and Resolution 45 (Rev. Dubai, 2014) and to reflect the current global state of play in the area of building confidence and security in the use of ICTs.

MOD IAP/46A19/1

RESOLUTION 50 (REV. HAMMAMET, 2016)

Cybersecurity

(Florianópolis, 2004; Johannesburg, 2008; Dubai, 2012, Hammamet, 2016)

The World Telecommunication Standardization Assembly (Hammamet, 2016),

recalling

*a)* Resolution 130 (Rev. Busan, 2014) of the Plenipotentiary Conference, on the role of ITU in building confidence and security in the use of information and communication technologies (ICT);

*b)* Resolution 174 (Rev. Busan, 2014) of the Plenipotentiary Conference, on ITU's role with regard to international public policy issues relating to the risk of illicit use of ICT;

*c)* Resolution 179 (Rev. Busan, 2014) 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 ICT;

*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.Dubai, 2012) of the World Telecommunication Development Conference (WTDC);

*j)* Resolution 52 (Rev. Dubai, 2012) of this assembly, on countering and combating spam;

*k)* Resolution 58 (Rev. Dubai, 2012) of this assembly, on encouraging the creation of national computer incident response teams, particularly in developing countries[[1]](#footnote-1)1,

considering

*a)* the crucial importance of 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;

*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; that the number and methods of cyberthreats and cyberattacks are growing, as is dependence on the Internet and other networks that are essential for accessing services and information;

*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 requiredto identify, prepare for, address and recover from cybersecurity incidents;

*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), as well as several consortia and standards entities such as the World Wide Web consortium (W3C), the Organization for Advancement of Structured Information Standards (OASIS), the Internet Engineering Task Force, and the Institute of Electrical and Electronics Engineers, among others, 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.Busan, 2014) 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 the WTDC-14 approved the contribution to the Strategic Plan of ITU for 2016-2019, endorsing five Objectives, among these Objective 3 – *Enhance confidence and security in the use of telecommunications/ICTs, as well as enhanced deployment of ICT applications and services*; and Outcome 3.1 of said Objective: *Improved confidence and security in the use of ICTs and services*, within whose framework of execution is the Cybersecurity Programme and Question 3/2 of the ITU Telecommunication Development Sector (ITU-D);

*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 cyberattack vectors such as phishing, pharming, scan/intrusion, distributed denials of service, web-defacements, unauthorized access, etc., are 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 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)* the significant and collaborative efforts by and among Governments, the private sector, civil society, the technical community and academia to build confidence and security in the use of information and communications technologies,

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 harden and defend information and telecommunication systems from cyberthreats and cyberattacks, 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 Question3/2;

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 Supplements thereto, 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 parties concerned are invited to work together to develop standards and guidelines in order to protect against cyberthreats and 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 Study Group 17 continue its work on the issues raised in Resolution 130 (Rev. Busan, 2014), and on the ITU‑T X-series of Recommendations, including Supplements as appropriate,

instructs the Director of the Telecommunication Standardization Bureau

1 tocontinue to maintian, 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 (Rev. Busan, 2014), 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 BDT in relation to any item concerning cybersecurity in accordance with Resolution 45 (Rev. Dubai, 2012),

3 taking into account Resolution 45 (Rev. Dubai, 2012), to support regional and global cybersecurity projects, such as, FIRST, OAS, APCERT, LAC-CSIRT, among others, and to invite all countries, particularly developing ones, to take part in these activities,

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.

1. 1 These include the least developed countries, small island developing states, landlocked developing countries and countries with economies in transition. [↑](#footnote-ref-1)