|  |  |  |  |
| --- | --- | --- | --- |
| itu_logo | World Telecommunication Standardization Assembly (WTSA-16) Hammamet, 25 October - 3 November 2016 | | CCITT/ITU-T 60th Anniversary logo |
|  | |  | |
|  | |  | |
| PLENARY MEETING | | Addendum 13 to Document 4202-E | |
|  | | 8 September 2016 | |
|  | | Original: English | |
|  | | | |
| Asia-Pacific Telecommunity Member Administrations | | | |
| APT COMMON Proposal for the work of the conference  REVISION OF WTSA-12 RESOLUTION 50  Cybersecurity | | | |

**Introduction**

Since WTSA-12, the ITU-T has made progress in cybersecurity-related activities. There have been some changes in cybersecurity threats landscape. There is a need for strengthening its activities and studying emerging security issues for the next Study Period (2017-2020).

It is necessary to update Resolution 50 to reflect the changes and developments that have occurred since 2012.

**Proposal**

APT Member Administrations would like to propose amendments to Resolution 50 on cybersecurity, as provided in Annex.

MOD APT/4202A13/1

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

*c)* Relevant resolutions of the United Nations General Assembly, including Resolution 57/239, Resolution 58/199 and Resolution 64/211, on the creation of a global culture of cybersecurity and the protection of essential information infrastructures;

*d)* Resolution 45 (Rev. Dubai, 2014) of the World Telecommunication Development Conference (WTDC), on mechanisms for enhancing cooperation on cybersecurity, including countering and combating spam;

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

*f)* 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 and their applications to practically all forms of social and economic activity including new development such as the Fourth Industrial Revolution (FIR) and internet of things;

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

*c)* that cybersecurity is a cross cutting issue, and that the cybersecurity landscape is complex and dispersed, with many different stakeholders at the national, regional and global levels with responsibility for identifying, examining and responding to issues related to building confidence and security in the use of ICTs;

*d)* that the ITU Telecommunication Standardization Sector (ITU-T) has adopted around 300 standards relating to building confidence and security in the use of ICTs;

*e)* the final report on Question 22-1/1 (Securing information and communication networks: Best practices for developing a culture of cybersecurity) of the ITU Telecommunication Development Sector (ITU-D);

*f)* that standardization work on security issues related to Internet of Things (IoT) and Smart Cities and Communities (SCC) applications that has impact on safety of internet users;

*g)* 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 for prevention, preparation, response and recovery from security incidents, and that the ITU-T has a role to play in this regard, within its mandate and competencies;

*h)* dynamic nature of global economy where supply of electronic and computing equipment constituting of vendor ecosystem is largely dispersed and critical in managing cyber security threats;

*i*) the work undertaken and ongoing in the ITU, including ITU-T Study Group 17, ITU-D Study Group 2 and under the Dubai Action Plan adopted by WTDC (Dubai, 2014);

*j)* that the ITU Telecommunication Standardization Sector (ITU‑T) has a role to play within its mandate and competencies in building confidence and security in the use of ICTs and *considering g)*,

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,

aware

*a)* that ITU-T 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, counterfeit devices, etc., and to protect personally identifiable information;

*b)* that ITU-T Study Group 17, ITU-D Study Groups 1 and 2 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. Dubai, 2012) and Resolutions 45 and 69 (Rev. Dubai, 2014);

*c)* that ITU-T is also assisting developing countries in building confidence and security in the use of ICTs and supporting the establishment of CIRTs, including CIRTs responsible for government-to-government cooperation, and the importance of coordination among all relevant organizations, in accordance with Resolutions 58 (Rev. Dubai, 2012),

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), and which was reaffirmed by the UN General Assembly High-Level Meeting on the overall review of the implementation of the outcomes of WSIS in December 2015;

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

*c)* 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)* the nature and type of cybersecurity incidents are many and varied (including but not limited to social engineering attack, advanced persistent threats, etc.), and continue to change over time, and that the sources of cybersecurity attacks are sometimes difficult to identify;

*b)* cybersecurity threats arise due to vulnerabilities in code, software and hardware which may be critical to national infrastructure and even harmful to human life, which requires timely vulnerability management and issuance of software/hardware patch when required;

*c)* data is becoming the key assets of the information and telecommunication networks as well as the main target of cybersecurity attacks,

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 identity management, 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 there is a role for ITU-D in assisting developing countries in cybersecurity capacity building activities to suit specific conditions and requirements of each country;

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

resolves

1 to continue to give this work high priority within ITU-T, in accordance with its competences and expertise, including promoting common understanding among governments and other stakeholders of building confidence and security in the use of ICTs at the national regional and international level;

2 that all ITU‑T study groups continue to evaluate existing, evolving and new Recommendations, with respect to their robustness of design and potential for exploitation by malicious parties, in particular new services and applications infrastructure (e.g. including but not limited to big data analytics, cloud computing, smart city, digital financial services, mobile edge computing, quantum computing, the 5th generation mobile networks, e-health, internet of things, software defined networking, network function virtualization, industrial internet, smart grid and intelligent transport systems, which are based on telecommunication/ICT networks such as IMT-2020) to be supported by the global telecommunication/ICT infrastructure, and report to TSAG as appropriate;

3 that ITU-T should start research on standards related to security of big data, focusing on whole lifecycle data protection and data security evaluation standards and practices;

4 that ITU‑T continue to raise awareness, within its mandate and competencies, 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;

5 that ITU‑T should work closely with ITU‑D, particularly in the context of Question3/2, Securing information and communication networks: Best practices for developing a culture of cybersecurity;

6 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;

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

8 that Study Group 17 in close collaboration with all other ITU‑T study groups establish an action plan to assess existing, evolving and new ITU-T Recommendations for security vulnerabilities and continue to provide regular reports on security of telecommunications/ICT to the Telecommunication Standardization Advisory Group (TSAG);

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 groups to address cybersecurity threat management that covers the roles and responsibilities of equipment provider, software provider, service provider and end users in ensuring cyber threat management is effective and provides a clear multi-party responsibility in mitigating cyber security threats;

11 that Study Group 17 continue its work on the technical means for the security of ICT networks, in particular relevant matters raised in Resolution 130 (Rev. Busan, 2014),

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 contribute to annual reports to the ITU Council on building confidence and security in the use of ICTs, as specified in Resolution 130 (Rev. Busan, 2014);

3 to publish the annual report on the progress of the activities of the “ICT Security Standards Roadmap” to ITU Council as specified in Resolution 130 (Rev. Busan, 2014) and evaluate theeffectiveness of the current works and plan for future works, direction or roadmap;4 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;

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

6 to cooperate with BDT in relation to any item concerning cybersecurity in particular the implementation of Resolution 45 (Rev. Dubai, 2014),

7 to continue to collaborate under the Global Cybersecurity Agenda (GCA) , as appropriate, to develop relationships and partnerships with various regional and international cybersecurity-related organizations and initiatives;

8 to encourage collaboration with ITU-D in their development of a cybersecurity management framework and principles for reference of Member States;

9 to identify and document practical steps to strengthen security in the use of ICTs internationally, based on widely accepted practices, guidelines and recommendations, that Member States can choose to apply to improve their ability to combat cyberthreats and attacks and to strengthen international cooperation in building confidence and security in the used of ICTs, taking into account the ITU Global Cybersecurity Agenda (GCA) and within the available financial resources,

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

1 to closely collaborate in strengthening regional and international cooperation, taking into account Resolution 130 (Rev. Busan, 2014) of the Plenipotentiary Conference, with the view to enhance confidence and security on the use of ICTs, in order to mitigate risks and threats;

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

3 to work together to develop cybersecurity standards and guidelines in order to protect against cyberattacks;

4 to utilise relevant ITU-T Recommendations, in particular the ITU-T X series of Recommendations and Supplements.

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