|  |  |  |
| --- | --- | --- |
| itu_logo | World Telecommunication Standardization Assembly (WTSA-16)Hammamet, 25 October - 3 November 2016 | CCITT/ITU-T 60th Anniversary logo |
|  |  |
|  |  |
| WORKING GROUP 4A | Document DT/83-E |
|  | 31 October 2016 |
|  | Original: English |
|  |
| Chairman of Ad Hoc Group |
| DRAFT REVISED RESOLUTION 50 CYBERSECURITY |
|  |
| **Chairman:** Jeferson Fued Nacif |

The TD reflects the outcome of the WG4A AHG on Res.50, 52, [ARB-6].

Square brackets exist

* on *considering further* *d)*;
* on *recognizing e)*;
* within *recognizing f)*;
* on *regcognizing g)*, and *h)*;
* within *resolves 3), and 8);*
* on *resolves 9).*

MOD ADHOC/83/1#37824

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 70/125 of the UNGA on the Outcome document of the high-level meeting of the General Assembly on the overall review of the implementation of the outcomes of the World Summit on the Information Society;

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

*k)* Resolution 52 (Rev. Hammamet, 2016) of this assembly, on countering and combating spam;

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

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

*n)* the cybersecurity-related provisions of the WSIS outcomes,

considering

*a)* the crucial importance of telecommunications/ICT infrastructure and their applications 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 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;

*f)* that the considerable and increasing losses which users of telecommunication/ICT systems have incurred from the growing problem of cybersecurity alarm all developed and developing nations of the world without exception;

*g)* that the fact, among others, that critical telecommunication/ICT infrastructures are interconnected at the global level means that inadequate infrastructure security in one country could result in greater vulnerability and risks in others, and therefore, cooperation is important;

*h)* 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;

*i)* that standards can support the security aspects of Internet of things (IoT) and Smart Cities and Communities (SCC);

*j)* 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 cyber security incidents;

*k*) the work undertaken and ongoing in the ITU, including ITU-T Study Group 17, ITU-D Study Group 2, including the final report of ITU-D SG1 Q22/1-1 and under the Dubai Action Plan adopted by WTDC (Dubai, 2014);

*l)* that the ITU Telecommunication Standardization Sector (ITU‑T) has a role to play within its mandate and competencies in *considering j)*,

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;

[*d)* the importance of security of distributed data considering their whole lifecycle;]

recognizing

*a)* the *instructs* TSB Director paragraph to intensify work within existing ITU-T study groups;

*b)* 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);

*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;

*d)* considering security aspects throughout the whole lifecycle of the standards development process;

*e)* that Recommendation ITU-T X.1255 ,which is based on the Digital Object Architecture, provides a framework for discovery of identity management information;

[that an identity management plays an important role in many telecommunications/ICT services and that it can be implemented using a range of technologies and solutions, including PKI and others;]

[*f)* the importance of a system which provides unique identification, assignment and resolution of digital objects including the use of handles and abstracts references;

*g)* the challenges that States, particularly in developing nations, face in building 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;

*d)* Noting that critical cybersecurity threats in software and hardware may require timely vulnerability management and timely hardware and software updates;

*e)* that securing data is a key component of cybersecurity as data is often the target in cyberattacks;

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

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)* the significant and collaborative efforts by and among governments, the private sector, civil society, the technical community and academia within their respective role and responsibilities to build confidence and security in the use of ICTs;

 *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 and evolving new Recommendations, with respect to their robustness of design and potential for exploitation by malicious parties, and take into account new services and emerging applications to be supported by the global telecommunication/ICT infrastructure (e.g. including but not limited to cloud computing and IoT, which are based on telecommunication/ICT networks), according to their mandates in Resolution 2;

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

4 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;

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

7 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 to counter security vulnerabilities and continue to provide regular reports on security of telecommunications/ICT to the Telecommunication Standardization Advisory Group (TSAG);

8 that ITU‑T study groups continue to liaise with standards organizations and other bodies active in this field;;

[9 that Study Group 3 continues its work on developing Recommendations, Technical Papers and other publications related to cybersecurity policy, regulatory and economic issues and their impact taking into account the emerging technologies including big data, cloud computing and the Internet of things (IoT);]

10 that security aspects are considered throughout the ITU-T standard development process,

instructs the Director of the Telecommunication Standardization Bureau

1 to continue to maintain, 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 report on the progress of the activities of the “ICT Security Standards Roadmap” to ITU Council;

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

7 to cooperate with the Secretary-General's Global Cybersecurity Agenda (CGA)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;

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

9 to support relevant ITU-T study group activities related to strengthening and building confidence and security in the use of ICTs,

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 participate in relevant ITU-T study group activities to develop cybersecurity standards and guidelines in order to build confidence and security in the use of ICTs;

4 to utilise relevant ITU-T 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)