|  |  |  |  |
| --- | --- | --- | --- |
| itu_logo | World Telecommunication Standardization Assembly (WTSA-16) Hammamet, 25 October - 3 November 2016 | | CCITT/ITU-T 60th Anniversary logo |
|  | |  | |
|  | |  | |
| PLENARY MEETING | | Addendum 24 to Document 42-E | |
|  | | 10 October 2016 | |
|  | | Original: English | |
|  | | | |
| African Telecommunication Union Administrations | | | |
| Proposed modification of Resolution 50 - Cybersecurity | | | |
|  | | | |

|  |  |
| --- | --- |
| **Abstract:** | This contribution proposes amendments to Resolution 50 to request 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), as well as the promise of the Digital Object Architecture (DOA) in enhancing cybersecurity. |

# 1 Introduction

Taking into account of the considerable and increasing losses which users of telecommunication/ ICT systems have incurred due to the growing problem of cybersecurity and deliberate sabotage worldwide, which alarms all developed and developing nations of the world without exception to take suitable actions towards a more trustworthy cyberspace. It is well noted that critical telecommunication/ICT infrastructures are interconnected at the global level, which means that low infrastructure security in one country could result in greater vulnerability and risks in others.

There is a need to take appropriate actions and preventive measures at the international level against the abusive uses of cyberspace, including telecommunication/ICT networks, as well as countering terrorism in all its forms and manifestations on cyberspace including telecommunication/ICT networks.

The importance of security, continuity and stability of telecommunication/ICT networks is obvious; the need to protect telecommunication/ICT networks from threats and vulnerabilities, while ensuring respect for privacy and the protection of personal information and data is a highly desirable target.

It is important to highlight the role of ITU 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.

It should be noted that the Digital Object Architecture (DOA) and one of its components, the Handle System, could enhance security and privacy in the cyberspace.

# 2 Proposal

Accordingly, the proposed amendments to Resolution 50 address the issues discussed above and we invite ITU-T Study Group 3 to 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), and we encourage ITU-T study groups continue to liaise with other SDOs and bodies, including the DONA Foundation.

MOD AFCP/42A24/1

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, 2014) 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;

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

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

*n)* that ITU and the United Nations Office on Drugs and Crime (UNODC) have signed a memorandum of understanding (MoU) in order to strengthen security in the use of ICTs,

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 the considerable and increasing losses which users of telecommunication/ICT systems have incurred from the growing problem of cybersecurity and deliberate sabotage worldwide, alarm all developed and developing nations of the world without exception;

*f)* that, among others, the fact that critical telecommunication/ICT infrastructures are interconnected at the global level means that low infrastructure security in one country could result in greater vulnerability and risks in others;

*g)* 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;

*h)* 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;

*i)* 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. 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 Programme 2, on cybersecurity, ICT applications and IP-based network related issues adopted by WTDC (Dubai, 2014) includes cybersecurity as one of its priority activities and relevant activities to be undertaken by the Telecommunication Development Bureau (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. Dubai, 2014), 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;

*e)* the need to take appropriate actions and preventive measures at the international level against the abusive uses of cyberspace, including telecommunication/ICT networks, the need to counter terrorism in all its forms and manifestations on cyberspace including telecommunication/ICT networks, the importance of the security, continuity and stability of telecommunication/ICT networks and the need to protect telecommunication/ICT networks from threats and vulnerabilities (§ 45 of the Tunis Agenda), while ensuring respect for privacy and the protection of personal information and data;

*f)* the role of ITU 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;

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

*h)* that the Handle System, which is a component of the DOA, has many benefits including storing the Handles as hierarchic Identifiers with secure access to attributes that must be authorized, management functions are self-contained and changes are controlled by the use of a Public Key Infrastructure (PKI) which is also self-contained in the system, and access to the Handle System may be signed and validated by the user,

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 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. Busan, 2014), a national IP-based public network security centre for developing countries is under study by 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 Supplements thereto,

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 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 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), the Internet Engineering Task Force (IETF), and the Digital Object Numbering Authority (DONA);

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;

11 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),

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 (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, 2014),

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. Busan, 2014), 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. Dubai, 2014)) 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.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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