**World Telecommunication Standardization Assembly 2012 (WTSA-12)**

**Addendum 2 to**

**Document WTSA/XXX**

**XXX XXX 2012**

**Original: English**

**European Common Proposals for the work of the Conference**

**MOD** EUR/XX/2

Resolution 50

Cybersecurity

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

The World Telecommunication Standardization Assembly (Dubai, 2012). *recalling*

WTSA-08 Resolution 52 (Johannesburg) Countering and combating spam, and

WTSA-08 Resolution 58 (Johannesburg) Encourage the creation of national computer incidence response teams, particularly in developing countries.

*considering*

1. the crucial importance of the information and communication technologies (ICT) infrastructure to practically all forms of social and economic activity ;
2. that the legacy public switched telehone network (PSTN) has a level of inherent security properties because of its hierarchical structure and buit-in management systems ;
3. that IP networks provide reduced separation between user components and network components if adequate care is not taken in security design and management ;
4. 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;
5. that the type and number of cyberincidents, including attacks from worms, viruses, malicious intrusions and thrill-seeker intrusions are on the increase.

*considering further*

1. that the Recommendation ITU-T X.1205 *‘Overview of Cybersecurity’* provides a definition, a description of technologies, and network protection principles;
2. that Recommendation ITU-T X.805 provides a systematic framework for identifying security vulnerabilities that, together with many new security-related deliverables from ITU and other organizations, can assist in risk assessment and in the development of mechanisms to mitigate risks ;
3. that the ITU Telecommunication Standardization Sector (ITU-T) and the Joint Technical Committee for Information Technology (JCT 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 taken into account.

*recognizing*

1. the relevant outcomes of the World Summit on the Information Society (WSIS) identified ITUas the facilitator and moderator for Action Line C5 (Building confidence and security in the use of ICTs) ;
2. the *resolves* paragraph of Resolution 130 (Rev. Guadalajara,2010) of 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 within the ITU study groups ;
3. that WTDC-10 has adopted the Hyderabad Action Plan and its Programme 3, on cybersecurity and ICT applications and IP-based network related issues, which identifies cybersecurity as a priority activity of the Telecommunication Development Bureau (BDT) and defines activities to be undertaken by BDT; and has also adopted Resolution 45 (Hyderabad, 2010), on mechanisms for enhancing cooperation on cybersecurity, including countering and combating spam;
4. 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*

1. that cyberattacks such as phishing, pharming, botnets, distributed denials of service etc, are emerging and having serious impacts ;
2. that the source of attack for spoofed IP addresses needs to be identifiable.

*noting*

1. the vigorous activity and interest in the development of security standards/ ICT standards and Recommendations in ITU-T Study Group 17, the lead ITU-T study group on telecommunication security, and in other standardization bodies, including the Global Standards Collaboration (GSC) group ;
2. 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 ;
3. that the cooperation and collaboration among organizations addressing security issues can promote progress and contribute to building and maintaining a culture of cybersecurity.

*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 designand potential for exploitation by malicious parties to interfere destructively with their deployment in the global information and telecommunication infrastructure ;
2. that ITU-T continue to raise awareness within the 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 the ITU-T should work closely with ITU-D, particularly in the context of Question 22/1 ;
4. that the ITU-T Recommendations, including X.805 and X.1205, ISO/IEC products/standards and other relevant deliverables from other organizations be used as a framework for assessing networks and protocols for security vulnerabilities and to share experiences ;
5. that concerned parties are invited to work together to develop standards and guidelines in order to protect against cyberattacks such as botnet, etc., and facilitate tracing the source of an attack ;
6. that global consistent and interoperable processes for sharing incident-response related information should be promoted ;
7. that all ITU-T study groups continues to provide regular reports on security of telecommunication/ ICT to the Telecommunication Standardization Advisory Group (TSAG) on progress in evaluating existing and evolving new Recommendations;
8. that ITU-T study groups continue to liaise with SDOs 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 Taskforce (IETF),

*instructs the Director of 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. Guadalajara,2010) on progress achieved in the actions outlined above.

*further instructs the Director of Telecommunication Standardization Bureau*

1. to continue to follow up WSIS cybersecurity activities 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 continue to cooperate with the Secretary-General’s initiative on cybersecurity, and with the Telecommunication Development Bureau in relation to any item concerning cybersecurity in accordance with WTDC Resolution 45 ( Hyderabad, 2010), and to ensure coordination among these different activities ;

3. to cooperate with all relevant international organisations and stakeholders who have international/ regional recognised experience of working on cybersecurity frameworks and issues, where appropriate,

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

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