|  |  |  |
| --- | --- | --- |
|  | World Telecommunication Standardization Assembly (WTSA-24)New Delhi, 15–24 October 2024 |  |
|  |
|  |  |
| PLENARY MEETING | Addendum 5 toDocument 38-E |
|  | 16 September 2024 |
|  | Original: English |
|  |
| Member States of European Conference of Postal and Telecommunications Administrations (CEPT) |
| PROPOSED MODIFICATION OF RESOLUTION 50 |
|  |
|  |

|  |  |
| --- | --- |
| **Abstract:** | CEPT proposes modifications to this Resolution to encourage joint work and to avoid duplication with other SDOs, to reduce the chance of the Resolution becoming outdated during the forthcoming study cycle, to further cement SG17’s role as the lead ITU-T study group for security issues, and to work more with regional telecommunications organisations, among other changes. It also proposes a change to clarify that security should be considered throughout the entire lifecycle of a system/network/application. |
| **Contact:** | Annie Norfolk BeadleDSITUnited Kingdom | E-mail: Annie.NorfolkBeadle@dsit.gov.uk |

MOD ECP/38A5/1

RESOLUTION 50 (Rev. New Delhi, 2024)

Cybersecurity

(Florianópolis, 2004; Johannesburg, 2008; Dubai, 2012; Hammamet, 2016; Geneva, 2022; New Delhi, 2024)

The World Telecommunication Standardization Assembly (New Delhi, 2024),

recalling

*a)* Resolution 130 (Rev. Bucharest, 2022) of the Plenipotentiary Conference, on the role of ITU in building confidence and security in the use of information and communication technologies (ICTs);

*b)* Resolution 174 (Rev. Dubai, 2018) of the Plenipotentiary Conference, on ITU's role with regard to international public policy issues relating to the risk of illicit use of ICTs;

*c)* Resolution 179 (Rev. Bucharest, 2022) 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 ICTs;

*e)* Resolutions 55/63 and 56/121 of the United Nations General Assembly (UNGA), which established the legal framework on countering the criminal misuse of information technologies;

*f)* UNGA Resolution 57/239, on the creation of a global culture of cybersecurity;

*g)* UNGA Resolution 58/199, on the creation of a global culture of cybersecurity and the protection of essential information infrastructures;

*h)* UNGA Resolution 41/65, on principles relating to remote sensing of the Earth from outer space;

*i)* UNGA Resolution 70/125, 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 (WSIS);

*j)* Resolution 45 (Rev. Kigali, 2022) 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 the World Telecommunication Standardization Assembly, on countering and combating spam;

*l)* Resolution 58 (Rev. Geneva, 2022) of this assembly, 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 telecommunication/ICT infrastructure and its application to practically all forms of social and economic activity;

*b)* that cybersecurity is a cross-cutting issue, and 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;

*c)* that the consequences of not taking adequate cybersecurity measures can affect all countries;

*d)* that the fact, *inter alia*, 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;

*e)* 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 standards can support the security aspects of all telecommunications/ICTs;

*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 in respect of cybersecurity incidents;

*h)* the work undertaken and ongoing in ITU, including in ITU Telecommunication Standardization Sector (ITU‑T) Study Group 17 and ITU Telecommunication Development Sector (ITU‑D) Study Group 2, and under the Kigali Action Plan adopted by WTDC (Kigali, 2022);

*i)* that ITU‑T has a role to play, within its mandate and competencies, in regard to *considering j)*,

considering further

*a)* that principle-based and risk-based approaches, information exchange and systemic vulnerability analysis can greatly improve the security of current and emerging technologies;

*b)* 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 (IETF) the Institute of Electrical and Electronics Engineers (IEEE), and the European Telecommunications Standards Institute (ETSI), 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;

*c)* the importance of considering security in the use of ICTs as a continuous and iterative process, built into products from the beginning and continuing throughout their lifetime;

*d)* that an iterative, risk-based approach incorporating a combination of technological, process, and human-based approaches is key to strengthening security and resilience in the use of ICTs – by enabling cybersecurity practices to be developed and applied as needed to address constantly evolving threats and vulnerabilities – while also supporting innovation and emerging telecommunications/ICTs,

recognizing

*a)* the operative paragraph of Resolution 130 (Rev. Bucharest, 2022) instructing the Director of the Telecommunication Standardization Bureau (TSB) to intensify work within existing ITU‑T study groups;

*b)* that Resolution 71 (Rev, Bucharest, 2022) of the Plenipotentiary Conference adopted the strategic plan for 2024-27, including ‘Inclusive and secure telecommunication/ICT infrastructure and services’ as one of five thematic priorities for the Union, and highlighting ‘enhanced capacity of the ITU membership to deploy inclusive, secure and resilient telecommunication/ICT infrastructures, to address cybersecurity-related incidents, to build confidence and security in the use of telecommunications/ICTs, and to adopt risk-management practices’ as a key outcome;

*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, considering security aspects throughout the whole lifecycle of the standards-development process;

*d)* the challenges that States, particularly in developing nations, face in building confidence and security in the use of ICTs,

recognizing further

*a)* that an increasing range and diversity of cyberattacks are emerging, evolving, and having significant impacts;

*b)* that a range of vectors may be used to distribute bot-malware and carry out cyberattacks;

*c)* that sources of attacks are sometimes difficult to identify;

*d)* 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 are 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 roles 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 competencies 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 (including, but not limited to, for example, cloud computing and IoT, which are based on telecommunication/ICT networks), according to their mandates in Resolution 2 (Rev. Geneva, 2022) of this assembly, and highlight any security concerns to Study Group 17;

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 malicious cyberactivity, 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 raise global awareness regarding security in ICTs through the development of Recommendations and technical reports which support cybersecurity procedures, technical policies and standards frameworks;

5 that ITU-T should take fully into account the importance of capacity building to facilitate the adoption of standards to support cybersecurity, particularly for developing countries, but not limited to them;

6 that ITU‑T should coordinate and collaborate with ITU‑D in this regards, both within the context of ITU-D Question 3/2 (Securing information and communication networks: Best practices for developing a culture of cybersecurity) and within the context of the BDT’s capacity building work;

7 that relevant ITU-T study groups should keep pace with the development of new and emerging technologies, according to their mandates, in order to alert Study Group 17 to areas that may require new Recommendations, supplements and technical reports to address challenges related to security;

8 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;

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

10 that ITU‑T study groups continue to liaise with standards organizations and other bodies active in this field and encourage the engagement of experts in ITU's activities in the area of building confidence and security in the use of ICTs;

11 that security aspects should be considered throughout the ITU‑T standards-development process;

12 that secure, trusted and resilient telecommunication/ICT networks and services should be developed and maintained to enhance confidence in the use of ICT;

13 that Study Group 17 should continue to support cooperative security analysis and tools for incident management, in order to support the work of CIRTs, particularly in developing countries;

14 that the resilience of ICT networks and systems should be considered as a priority in network and infrastructure development,

instructs Study Group 17

1 to promote studies on cybersecurity, including security for new services and emerging applications to be supported by the global telecommunication/ICT infrastructure;

2 to support the Director of TSB to maintain the ICT Security Standards Roadmap, which should include work items to progress standardization work related to security, and share this with relevant groups of the ITU Radiocommunication Sector (ITU-R) and ITU-D as the mission of the lead group for security;

3 to lead joint coordination activities on security among all relevant study groups and focus groups in ITU and other standards-development organizations, as appropriate;

4 to develop an action plan for joint work with other standards development organizations, with measurable targets that can be monitored over the forthcoming study cycle, and to report on performance against this action plan to TSAG on at least an annual basis;

5 to collaborate closely with all other ITU-T study groups, establish an action plan for assessing 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;

6 to develop a common approach towards the gap analysis exercise required for new work items, working with other SDOs (such as ISO, IEC, W3C, OASIS, IETF, IEEE, and ETSI) as well as partners in the security ecosystem that have specific knowledge and expertise in provisioning security for network/applications and services, and to submit this to TSAG for approval and publication on the ITU website;

7 to define a general/common set of security capabilities for each phase of information system/network/application lifecycles, so that consequently security could be achieved for systems/networks/applications from day one and continue throughout system/network/application lifecycles;

8 to design one or more security architecture reference frameworks with security functional components which could be considered as the basis of security architecture design for various systems/networks/applications in order to improve the quality of Recommendations on security,

instructs the Director of the Telecommunication Standardization Bureau

1 to continue to contribute to the ITU’s ongoing mapping and signposting work and to support efforts to engage other standards setting bodies in this process – in order to provide countries with more information on standards setting work in this important field;

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. Dubai, 2018);

3 to report to the Council on the progress of activities on the ICT Security Standards 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 the other ITU Sectors and in cooperation with other organisations and all relevant stakeholders, as a way to share information and best practices on national, regional and international non-discriminatory cybersecurity-related initiatives globally;

6 to cooperate with the Secretary-General's GCA and other global or regional cybersecurity projects, as appropriate, in promoting capacity building and developing 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;

7 to support the Director of the Telecommunication Development Bureau (BDT) in overseeing the development of Recommendations and potentially other tools that the Member States, particularly developing countries, can use to anticipate rapid responses in case of major incidents, and in helping these bodies to develop action plans to increase their protection, taking into account mechanisms and partnerships, as appropriate;

8 to support relevant Study Group 17 activities related to strengthening and building confidence and security in the use of ICTs, and to coordinate this work with that of the ITU-D study groups and with the relevant programme activities;

9 to disseminate information to all stakeholders related to cybersecurity through the organization of training programmes, forums, workshops, seminars, etc., for policy-makers, regulators, operators and other stakeholders, especially from developing countries, to raise awareness and identify needs in collaboration with the Director of BDT;

10 to work with the Regional Telecommunications Organisations to deliver knowledge, tools, and expertise to wider audiences more effectively,

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

1 to collaborate closely in strengthening regional and international cooperation and support, taking into account Resolution 130 (Rev. Bucharest, 2022), with a view to enhancing confidence and security in 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 utilize 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)