|  |  |  |
| --- | --- | --- |
| ITU logo | INTERNATIONAL TELECOMMUNICATION UNION**TELECOMMUNICATIONSTANDARDIZATION SECTOR**STUDY PERIOD 2017-2020 | TSAG-TD1288 |
| TSAG |
| **Original: English** |
| **Question(s):** | N/A | Virtual, 10-17 January 2022 |
| **TD** |
| **Source:** | Rapporteur, RG-WP |
| **Title:** | WTSA Resolution 50 proposals side-by-side |
| **Purpose:** | Information, Discussion |
| **Contact:** | Miho NaganumaNEC CorporationJapan | E-mail: m\_naganuma@nec.com  |

|  |  |
| --- | --- |
| **Keywords:** | WTSA Resolution 50; |
| **Abstract:** | This TD provides the contact/focal points for WTSA Resolution 50, and the proposals in a side-by-side view. |

**Contact/focal points:**

|  |  |  |  |
| --- | --- | --- | --- |
| **RTO** | **Proposal type** | **Contact(s)/focal point(s)** | **e-mail address** |
| **APT** | MOD | Zhaoji Lin | lin.zhaoji@zte.com.cn  |
| Nadia Hazwani Yaakob | nadiahazwani.yaakob@mcmc.gov.my  |
| Heung Youl YOUM | hyyoum@sch.ac.kr  |
| **AST** | MOD | Abdulaziz Alfaiz | afaiz@citc.gov.sa  |
| **ATU** | MOD | Ahmed Gharbi | ahmed.gharbi@cert.mincom.tn  |
| Evah Kentshitswe | kentshitswe@bocra.org.bw  |
| Sana Souai | sana.souai@anf.tn  |
|  |  |
| **CEPT** | MOD | Irfan Hermani | irfan.hemani@dcms.gov.uk  |
| **CITEL** | MOD | João Alexandre Zanon | zanon@anatel.gov.br  |
| **RCC** | MOD | Evgeny Tonkikh | et@niir.ru  |
| **TSB** | --- | Xiaoya Yang | xiaoya.yang@itu.int  |

**Resolution 50 proposals side-by-side**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **PROPOSAL 1 (MOD,** [**WTSA C-037\_APT\_Add08**](https://www.itu.int/dms_pub/itu-t/md/17/wtsa.20/c/T17-WTSA.20-C-0037%21A8%21MSW-E.docx)**) (APT)** | **PROPOSAL 2 (MOD) (AST)** | **PROPOSAL 3 (MOD,** [**WTSA C-035 ATU Add09**](https://www.itu.int/dms_pub/itu-t/md/17/wtsa.20/c/T17-WTSA.20-C-0035%21A9%21MSW-E.docx)**) (ATU)** | **PROPOSAL 4 (MOD**[**, WTSA C-038\_ECP\_Add06**](https://www.itu.int/dms_pub/itu-t/md/17/wtsa.20/c/T17-WTSA.20-C-0038%21A6%21MSW-E.docx)**) (CEPT)** | **Proposal 5 (MOD,**[**WTSA-C-039\_IAP\_Add30**](https://www.itu.int/dms_pub/itu-t/md/17/wtsa.20/c/T17-WTSA.20-C-0039%21A30%21MSW-E.docx)**) (CITEL)** | **Proposal 6 (MOD,** [**TSAG-C187**](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T17-TSAG-C-0187)**-R1) (RCC)** |
| MOD APT/37A8/1**#71**RESOLUTION 50 (Rev. Geneva, 2022)Cybersecurity(Florianópolis, 2004; Johannesburg, 2008; Dubai, 2012; Hammamet, 2016; Geneva, 2022)The World Telecommunication Standardization Assembly (Geneva, 2022),recalling*a)* Resolution 130 (Rev. Dubai, 2018) 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. Dubai, 2018) 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 (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)* UNGA Resolution 71/199 on the right to privacy in the digital age;*k)* Resolution 45 (Rev. Dubai, 2014) of the World Telecommunication Development Conference (WTDC), on mechanisms for enhancing cooperation on cybersecurity, including countering and combating spam;*l)* Resolution 52 (Rev. Geneva, 2022) of this assembly, on countering and combating spam;*m)* Resolution 58 (Rev. Dubai, 2012) of the World Telecommunication Standardization Assembly, on encouraging the creation of national computer incident response teams, particularly in developing countries[[1]](#footnote-1)1;*n)* 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);*o)* the cybersecurity-related provisions of the WSIS outcomes,considering*a)* the crucial importance of telecommunication/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 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 and malicious cyber activities 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, *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;*h)* that the number and methods of cyberthreats and malicious cyber activity are growing day to day, and it is a challenging task to protect networks and systems from them as is dependence on the Internet and other networks that are essential for accessing services and information;*i)* that standards can support the security and security related aspects of Internet of things (IoT) and smart cities and communities (SC&C);*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 in respect of cybersecurity incidents;*k*) the work undertaken and ongoing in the ITU, including ITU Telecommunication Standardization Sector (ITU‑T) Study Group 17, ITU Telecommunication Development Sector (ITU‑D) Study Group 2, including the final report of ITU‑D Study Group 1 Question 22/1-1, and under the Dubai Action Plan adopted by WTDC (Dubai, 2014);*l)* that ITU‑T has a role to play, within its mandate and competencies, in regard to *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, Recommendation ITU‑T X.509 provides the Public-key and attribute certificate frameworks, 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 Fast IDentity Online (FIDO) alliance, the Internet Engineering Task Force (IETF), and the Institute of Electrical and Electronics Engineers (IEEE), 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 ongoing work on security reference architecture for lifecycle management of e‑commerce business data,recognizing*a)* the operative paragraph of Resolution 130 (Rev. Dubai, 2018) of the Plenipotentiary Conference instructing the Director of the Telecommunication Standardization Bureau (TSB) to intensify work within existing ITU‑T study groups; *b)* that WTDC-14 approved the contribution to the strategic plan of the Union for 2016-2019, endorsing five Objectives, among them Objective 3 – *Enhance confidence and security in the use of telecommunications/ICTs, and roll-out of relevant ICT applications and services*, and the associated Output 3.1 – *Building confidence and security in the use of ICTs,* within whose framework of execution is the Cybersecurity Programme and ITU‑D Question 3/2;*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 cybersecurity incidence or cyber crime 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 cyber crimes;*c)* that sources of malicious cyber activities are sometimes difficult to identify; *d)* that some malicious cyber activities are caused by systems and devices that are connected to telecom networks without adequate authentication;*e)* that unauthorized access to ICT systems can be reduced by introducing emerging technologies such as distributed ledger technology that permit the access of any smart device to the network only after a validation process;*f)* that critical cybersecurity threats in software and hardware may require timely vulnerability management and timely hardware and software updates;*g)* that securing data is a key component of cybersecurity as data are often the target in malicious cyber activity;*h)* that cybersecurity is one of the elements for building confidence and security in the use of telecommunications/ICTs;*i)* that security occupies an important position throughout the lifecycle of systems/ networks/ applications/ data;*j* that common security architecture(s) is important and could be considered as the basis of security architecture for various systems/networks/applications/data,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,resolves1 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 (e.g. including, but not limited to, cloud computing, distributed ledger technology, quantum-based security, and IoT, which are based on telecommunication/ICT networks), according to their mandates in Resolution 2 (Rev. Geneva, 2022) of this assembly;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 cyber activity, 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 ITU-D Question 3/2 (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 ITU‑T study groups continue to liaise with standards organizations and other bodies active in this field;8 that security aspects are considered throughout the ITU‑T standards-development process;9 that the specifications and standards to test and certify the security of ICT systems are developed to build confidence among users and to assist in setting up test-beds and test labs, especially in developing countries;10 that secure, trusted and resilient telecommunication/ICT networks and services should be developed and maintained to enhance confidence in the use of ICT,instructs Study Group 17 1 to promote the 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 the Telecommunication Standardization Bureau 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 ITU-R and ITU-D as the mission of the lead group for security; 3 to establish the Joint Coordination Activity for security (JCA Security) and coordinate the standardization activities of security among all relevant study groups and focus groups in ITU and other SDOs;4 to collaborate closely with all other ITU T study groups, to 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);5 to define a general/common set of security capabilities for each phase of information systems/networks/applications/data lifecycle, so that consequently intrinsic security (security capabilities and features available by design) could be achieved for systems/networks/applications/data from day one;6 to design common security architecture(s) with security functional components which could be considered as the basis of security architecture design for various systems/networks/applications/data in order to improve the quality of recommendations on security,instructs the Director of the Telecommunication Standardization Bureau1 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, including the development of common approaches in the field of cybersecurity; 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) of the Plenipotentiary Conference;3 to report to the Council on the progress of the 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 relevant stakeholders, as a way to share information 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, 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;7 to support the Director of the Telecommunication Development Bureau in assisting Member States in the establishment of an appropriate framework among 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;8 to support relevant ITU‑T study group activities related to strengthening and building confidence and security in the use of ICTs;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,invites Member States, Sector Members, Associates and academia, as appropriate1 to closely collaborate in strengthening regional and international cooperation, taking into account Resolution 130 (Rev. Dubai, 2018) of the Plenipotentiary Conference, with a view to enhancing confidence and security in the use of ICTs, in order to mitigate cyber risks and cyber threats; 2 to cooperate and participate actively in the implementation of this resolution and the associated actions, including review and updating of their cyber security architectures and protocols design;3 to participate in relevant ITU‑T study group activities to develop cybersecurity standards and guidelines in order to build confidence and security through data protection and security mechanisms in the use of ICTs; 4 to utilize relevant ITU‑T Recommendations and Supplements;5 to develop cyber risk management mechanisms to recover any loss and damage from malicious cyber activity such as cyber insurance as part of cyber security practices. |  | MOD AFCP/35A9/1**#99**RESOLUTION 50 (Rev. Geneva, 2022)Cybersecurity(Florianópolis, 2004; Johannesburg, 2008; Dubai, 2012; Hammamet, 2016; Geneva, 2022)The World Telecommunication Standardization Assembly (Geneva, 2022),recalling*a)* Resolution 130 (Rev.  Dubai, 2018) 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.  Dubai, 2018) 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 (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)* UNGA resolution 75/240 decides that the open-ended working group on security of and in the use of information and communications technologies 2021–2025 shall start its activities upon the conclusion of the work of the current Open-ended Working Group and considering its outcomes;*k)* UNGA 74/247 on the Ad hoc committee to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes;*l)* Resolution 45 (Rev. Dubai, 2014) of the World Telecommunication Development Conference (WTDC), on mechanisms for enhancing cooperation on cybersecurity, including countering and combating spam;*m)* Resolution 52 (Rev. Hammamet, 2016) of this assembly, on countering and combating spam;*n)* Resolution 58 (Rev. Dubai, 2012) of the World Telecommunication Standardization Assembly, on encouraging the creation of national computer incident response teams, particularly in developing countries[[2]](#footnote-2)1;*o)* 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);*p)* the cybersecurity-related provisions of the WSIS outcomes,considering*a)* the crucial importance of telecommunication/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 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, *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;*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 (SC&C);*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 in respect of cybersecurity incidents;*k*) the work undertaken and ongoing in the ITU, including ITU Telecommunication Standardization Sector (ITU‑T) Study Group 17, ITU Telecommunication Development Sector (ITU‑D) Study Group 2, including the final report of ITU‑D Study Group 1 Question 22/1-1, and under the Dubai Action Plan adopted by WTDC (Dubai, 2014);*l)* that ITU‑T has a role to play, within its mandate and competencies, in regard to *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 (IETF), and the Institute of Electrical and Electronics Engineers (IEEE), 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 ongoing work on security reference architecture for lifecycle management of e‑commerce business data,recognizing*a)* the operative paragraph of Resolution 130 (Rev. Dubai, 2018) instructing the Director of the Telecommunication Standardization Bureau (TSB) to intensify work within existing ITU‑T study groups; *b)* that WTDC-14 approved the contribution to the strategic plan of the Union for 2016-2019, endorsing five Objectives, among them Objective 3 – *Enhance confidence and security in the use of telecommunications/ICTs, and roll-out of relevant ICT applications and services*, and the associated Output 3.1 – *Building confidence and security in the use of ICTs,* within whose framework of execution is the Cybersecurity Programme and ITU‑D Question 3/2;*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 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)* 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,resolves1 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 (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 (Rev. Hammamet, 2016) of this assembly;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 ITU-D Question 3/2 (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 security aspects are considered throughout the ITU‑T standards-development process;10 that ITU-T study group 17 need to give high priority to digital forensics investigation, following the recommendation ITU-T X.1056 on security incident management guidelines for telecommunications organizations; and X.1060 on Framework for the creation and operation of a Cyber Defence Centre,instructs the Director of the Telecommunication Standardization Bureau1 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.  Dubai, 2018);3 to report to the Council on the progress of the 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 relevant stakeholders, as a way to share information and best practices on critical and network infrastructure security and how to mitigate current and new threats 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, 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;7 to support the Director of the Telecommunication Development Bureau in assisting Member States in the establishment of an appropriate framework among 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;8 to cooperate within the Secretary-General’s GCA in promoting capacity building on cyber security for all member States particularly developing countries by inviting cyber security entities to cooperate with the Secretary-General's GCA to deploy regional cyber security centers of excellence to train, educate and raise awareness on cyber security domains such as (technical, strategic, law enforcement, investigation, digital evidence, and cooperation ……)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 appropriate1 to closely collaborate in strengthening regional and international cooperation, taking into account Resolution 130 (Rev.  Dubai, 2018), 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. | MOD EUR/38A6/1**#13**RESOLUTION 50 (Rev. Geneva, 2022)Cybersecurity(Florianópolis, 2004; Johannesburg, 2008; Dubai, 2012; Hammamet, 2016;Geneva, 2022)The World Telecommunication Standardization Assembly (Geneva, 2022),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 (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 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);*i)* Resolution 45 (Rev. Dubai, 2014) of the World Telecommunication Development Conference (WTDC), on mechanisms for enhancing cooperation on cybersecurity, including countering and combating spam;*j)* Resolution 52 (Rev. Hammamet, 2016) of this assembly, on countering and combating spam;*k)* Resolution 58 (Rev. Dubai, 2012) of the World Telecommunication Standardization Assembly, on encouraging the creation of national computer incident response teams, particularly in developing countries[[3]](#footnote-3)1;*l)* 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);*m)* the cybersecurity-related provisions of the WSIS outcomes,considering*a)* the crucial importance of telecommunication/ICT infrastructure and their applications 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 considerable harm which may be incurred through inadequate security of ICTs alarm all developed and developing nations of the world without exception;*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 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 the ITU, including ITU Telecommunication Standardization Sector (ITU‑T) Study Group 17, ITU Telecommunication Development Sector (ITU‑D) Study Group 2 and under the Dubai Action Plan adopted by WTDC (Dubai, 2014);*i)* that ITU‑T has a role to play, within its mandate and competencies, in regard to *considering g)*,considering further*a)* that principle-based approaches, information and exchange and systematic vulnerability analysis can greatly improve the security of all 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), and the Institute of Electrical and Electronics Engineers (IEEE), 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, including in relation to security reference architecture for lifecycle management of e‑commerce business data;*d*) that a risk-based approach incorporating a combination of technological, process, and people-based approaches can assist in strengthening security and resilience in the use of ICTs,recognizing*a)* the operative paragraph of Resolution 130 (Rev. Busan, 2014) instructing the Director of the Telecommunication Standardization Bureau (TSB) to intensify work within existing ITU‑T study groups; *b)* that Resolution 71 (Rev, Dubai 2018) adopted the Strategic Plan for 2020-23, including Strategic Goal 3 *Sustainability: Manage emerging risks, challenges and opportunities resulting from the rapid growth of telecommunications/ICT*, under which the Union will focus on enhancing the quality, reliability, sustainability and resilience of networks and systems as well as 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, 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 and having serious impacts; *b)* that a range of vectors may be used to distribute 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,resolves1 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 (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 (Rev. Hammamet, 2016) of this assembly;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 coordinate and collaborate closely with ITU‑D, particularly in the context of ITU-D Question 3/2 (Securing information and communication networks: Best practices for developing a culture of cybersecurity);5 that global, consistent and interoperable processes for sharing incident-response related information should be promoted;6 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);7 that study groups take into account the impact of the deployment of emerging technologies on cybersecurity, and incorporate this consideration in their activities;8 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 the ITU's activities in the area of building confidence and security in the use of ICTs;9 that security aspects are considered throughout the ITU‑T standards-development process,instructs the Director of the Telecommunication Standardization Bureau1 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 to the Council on the progress of the 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 relevant stakeholders, as a way to share information 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, 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;7 to support the Director of the Telecommunication Development Bureau in assisting Member States in the establishment of an appropriate framework among 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;8 to support relevant ITU‑T study group activities related to strengthening and building confidence and security in the use of ICTs and coordinate this work with that of the ITU-D study groups and with the relevant programme activities,invites Member States, Sector Members, Associates and academia, as appropriate1 to closely collaborate in strengthening regional and international cooperation, taking into account Resolution 130 (Rev. Busan, 2014), 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. | MOD IAP/39A30/1**#95**RESOLUTION 50 (Rev. Geneva, 2022)Cybersecurity(Florianópolis, 2004; Johannesburg, 2008; Dubai, 2012; Hammamet, 2016; Geneva, 2022)The World Telecommunication Standardization Assembly (Geneva, 2022),recalling*a)* Resolution 130 (Rev. Dubai, 2018) 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. 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 ICT;*c)* Resolution 179 (Rev. Dubai, 2018) 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 (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 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);*i)* Resolution 45 (Rev. Dubai, 2014) of the World Telecommunication Development Conference (WTDC), on mechanisms for enhancing cooperation on cybersecurity, including countering and combating spam;*j)* Resolution 52 (Rev. Hyderabad, 2020) of this assembly, on countering and combating spam;*k)* Resolution 58 (Rev. Dubai, 2012) of the World Telecommunication Standardization Assembly, on encouraging the creation of national computer incident response teams, particularly in developing countries[[4]](#footnote-4)1;*l)* 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);*m)* the cybersecurity-related provisions of the WSIS outcomes,considering*a)* the crucial importance of telecommunication/ICT infrastructure and their applications 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 considerable harm which may be incurred through inadequate security of ICTs alarm all developed and developing nations of the world without exception;*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)* that to protect the global telecommunication/ICT environment, ITU members should consider a set of minimum requirements at a national level, in order to coexist internationally, and procedures developed through ITU-T Recommendations and studies, as well as other recognized standards organizations;*i*) the work undertaken and ongoing in the ITU, including ITU Telecommunication Standardization Sector (ITU‑T) Study Group 17, ITU Telecommunication Development Sector (ITU‑D) Study Group 2 and under the Buenos Aires Action Plan adopted by WTDC (Buenos Aires, 2017);*j)* that ITU‑T has a role to play, within its mandate and competencies, in regard to *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, Recommendation ITU T X.509 provides the Public-key and attribute certificate frameworks, 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 (IETF), and the Institute of Electrical and Electronics Engineers (IEEE), 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 considering security in the use of ICTs as a continuous and iterative process, that is built into digital products and services from the design and continuing throughout their lifetime, and with due consideration of the risk associated with security breaches, including ongoing work on security reference architecture for lifecycle management of e‑government, e-b-business, e-commerce and other e-society services,recognizing*a)* the operative paragraph of Resolution 130 (Rev. Dubai, 2018) instructing the Director of the Telecommunication Standardization Bureau (TSB) to intensify work within existing ITU‑T study groups; *b)* that Resolution 71 (Dubai, 2018) adopted the Strategic Plan for 2020-2023, including Strategic Goal 3 *Sustainability: Manage emerging risks, challenges and opportunities resulting from* the *rapid growth* of *telecommunications/ICT*, under which the Union will focus on enhancing the quality, reliability, sustainability and resilience of networks and systems as well as building *confidence and security in the use of 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, 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 increasing range and diversity of cyberattacks such as phishing, pharming, scan/intrusion, distributed denials of service, web-defacements, unauthorized access, etc., are emerging and having serious 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,resolves1 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 (e.g. including, but not limited to, cloud computing, quantum-based security and IoT, which are based on telecommunication/ICT networks), according to their mandates in Resolution 2 (Rev. Geneva, 2022) of this assembly;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 raise global awareness and highlight national strategies and approaches regarding security in ICTs through the development of Recommendations and technical reports;5 that ITU‑T should coordinate and collaborate closely with ITU‑D, particularly in the context of ITU-D Question 3/2 (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 to counter 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 organizations and other bodies active in this field;10 that security aspects are considered throughout the ITU‑T standards-development process,instructs the Director of the Telecommunication Standardization Bureau1 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. Dubai, 2018);3 to report to the Council on the progress of the 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 relevant stakeholders, as a way to share information 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, 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;7 to support the Director of the Telecommunication Development Bureau in assisting Member States in the establishment of an appropriate framework among 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;8 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 appropriate1 to closely collaborate in strengthening regional and international cooperation, taking into account Resolution 130 (Rev. Dubai, 2018), 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. | MOD RESOLUTION 50 (Rev. Geneva2022)Cybersecurity(Florianópolis, 2004; Johannesburg, 2008; Dubai, 2012; Hammamet, 2016; Geneva, 2022)The World Telecommunication Standardization Assembly (Geneva2022),recalling*a)* Resolution 130 (Rev. Dubai, 2018) 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.  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 ICT;*c)* Resolution 179 (Rev.  Dubai, 2018) 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 (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. 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 the World Telecommunication Standardization Assembly, on countering and combating spam;*l)* Resolution 58 (Rev. Dubai, 2012) of the World Telecommunication Standardization Assembly, on encouraging the creation of national computer incident response teams, particularly in developing countries[[5]](#footnote-5)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 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 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, *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;*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 (SC&C), critical information infrastructure, including energy, transport, health, urban and rural spatial planning, agriculture, emergency, crisis and disaster management, public safety;*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 in respect of cybersecurity incidents;*k*) the work undertaken and ongoing in the ITU, including ITU Telecommunication Standardization Sector (ITU‑T) Study Group 17, ITU Telecommunication Development Sector (ITU‑D) Study Group 2, including the final report of ITU‑D Study Group 1 Question 22/1-1, and under the Dubai Action Plan adopted by WTDC (Dubai, 2014);*l)* that ITU‑T has a role to play, within its mandate and competencies, in regard to *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 (IETF), and the Institute of Electrical and Electronics Engineers (IEEE), 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 ongoing work on security reference architecture for lifecycle management of e‑commerce business data,recognizing*a)* the operative paragraph of Resolution 130 (Rev. Busan, 2014) instructing the Director of the Telecommunication Standardization Bureau (TSB) to intensify work within existing ITU‑T study groups; *b)* that WTDC-14 approved the contribution to the strategic plan of the Union for 2016-2019, endorsing five Objectives, among them Objective 3 – *Enhance confidence and security in the use of telecommunications/ICTs, and roll-out of relevant ICT applications and services*, and the associated Output 3.1 – *Building confidence and security in the use of ICTs,* within whose framework of execution is the Cybersecurity Programme and ITU‑D Question 3/2;*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 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)* that critical cybersecurity threats in software and hardware may require timely vulnerability management and timely hardware and software updates;*e)* that securing data, personal data and critical information infrastructure are a key components of cybersecurity system 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,resolves1 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 (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 (Rev. Hammamet, 2016) of this assembly;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 ITU-D Question 3/2 (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 security aspects are considered throughout the ITU‑T standards-development process,instructs the Director of the Telecommunication Standardization Bureau1 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. Dubai, 2018);3 to report to the Council on the progress of the 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 relevant stakeholders, as a way to share information 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, 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;7 to support the Director of the Telecommunication Development Bureau in assisting Member States in the establishment of an appropriate framework among 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;8 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 appropriate1 to closely collaborate in strengthening regional and international cooperation, taking into account Resolution 130 (Rev. Dubai, 2018), 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)
2. 1 These include the least developed countries, small island developing states, landlocked developing countries and countries with economies in transition. [↑](#footnote-ref-2)
3. 1 These include the least developed countries, small island developing states, landlocked developing countries and countries with economies in transition. [↑](#footnote-ref-3)
4. 1 These include the least developed countries, small island developing states, landlocked developing countries and countries with economies in transition. [↑](#footnote-ref-4)
5. 1 These include the least developed countries, small island developing states, landlocked developing countries and countries with economies in transition. [↑](#footnote-ref-5)