|  |  |
| --- | --- |
| **Plenipotentiary Conference (PP-18)Dubai, 29 October – 16 November 2018** |  |
|  |  |
|  |  |
| PLENARY MEETING | **Document 67-E** |
|  | **12 October 2018** |
|  | **Original: English** |
|  |
| Brazil (Federative Republic of) |
| Proposals for the work of the conference |
|  |
|  |

MOD B/67/1

RESOLUTION 14 (Rev. Dubai, 2018)

Recognition of the rights and obligations of all Sector Members of the Union

The Plenipotentiary Conference of the International Telecommunication Union (Dubai, 2018),

considering

*a)* that the rights and obligations of Member States and Sector Members of the Union are set out in Article 3 of the ITU Constitution;

*b)* that Article 19 of the ITU Convention lists the types of entities and organizations which may be authorized to participate in the activities of the Sectors as Sector Members;

*c)* that, except for the provisions of Nos 239 and 340C of the Convention, only Member States have the right to vote, particularly for the approval of recommendations and questions, in accordance with Article 3 of the Constitution,

recognizing

that Sector Members referred to in the lists established by the Secretary-General in accordance with No. 237 of the Convention may participate in all activities of the Sector concerned, with the exception of formal votes and some treaty-making conferences, and in this regard each Sector Member is entitled to:

a) receive from the Bureau of that Sector all the documents which they have requested relating to the Sector’s study groups, assemblies or conferences in which they may participate under the relevant provisions of the Convention and under the working methods and procedures of the Sector concerned;

b) send contributions to study groups, notably those in which they have requested to participate in due time, in accordance with the Sector’s working methods and procedures;

c) send representatives to such meetings, after having announced their names to the Bureau in due time, in accordance with the Sector’s working methods and procedures;

d) propose items for inclusion in the agendas of such meetings, except in relation to the structure and functioning of the Union;

e) take part in all discussions, and assume responsibilities such as chairmanship or vice-chairmanship of a study group, working party, expert group, rapporteur’s group or any other ad hoc group, according to the competence and availability of its experts;

f) take part in the drafting work and editorial work necessary prior to the adoption of recommendations,

recognizing further

that coordination between Member States and Sector Members at the national level has proved to increase the efficiency of the work,

resolves

to allow Sector Members to take part in any decision-finding procedure aimed at facilitating the achievement of a consensus in study groups, regional groups, working parties, advisory groups, regional workshops and meetings, and other activities, in particular in the field of standardization,

invites the world telecommunication development conference, radiocommunication assembly and world telecommunication standardization assembly

to adopt respective provisions in the working methods and procedures of their Sectors,

invites administrations of Member States

to conduct, at the national level, broad coordination among all Sector Members from their countries.

**Reasons:** Brazil proposes modifications to Resolutions 14 (Rev. Antalya, 2006) with the main objective of encouraging and facilitating the participation of ITU’s diverse membership in the many forums of discussion.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

MOD B/67/2

RESOLUTION 71 (Rev. Dubai, 2018)

Strategic plan for the Union for 2020-2023

The Plenipotentiary Conference of the International Telecommunication Union (Dubai, 2018),

considering

the provisions of the ITU Constitution and ITU Convention relating to strategic policies and plans,

noting

*a)* the challenges faced by the Union in achieving its purposes in the constantly changing telecommunication/information and communication technology (ICT) environment as well as the context for the development and implementation of the strategic plan, as outlined in Annex 1 to this resolution;

*b)* the glossary of terms presented in Annex 3 to this resolution,

recognizing

*a)* the experience gained in implementing the strategic plan for the Union for 2016-2019;

*b)* that the role of the regional presence in achieving “One ITU” should be mainstreamed in the Strategic Plan of the Union, and that the Council should ensure that this role is appropriately cascaded down into the operational plans of each Sector;

*c)* that the effective linkage between the strategic plan and the financial plan, which is detailed in Annex 1 to Decision 5 (Rev. Dubai, 2018) of this conference, can be achieved through reallocation of the resources of the financial plan to the various Sectors, and then to the goals and objectives of the strategic plan, as presented in the Appendix to Annex 1 to this resolution,

resolves

to adopt the Strategic Plan for the Union for 2020-2023, contained in Annex 1 to this resolution,

instructs the Secretary-General and the Coordination Committee

1 to further develop and implement an ITU results framework for the Strategic Plan of the Union for 2020-2023 (Annex 1), following the principles of results-based management (RBM) and results-based budgeting (RBB);

2 to coordinate the implementation of the strategic plan, ensuring coherence between the strategic plan, the financial plan, the operational plans and the biennial budgets;

3 to annually report to the ITU Council on the implementation of the strategic plan for 2020-2023 and on the performance of the Union towards the achievement of its goals and objectives;

4 to recommend to the ITU Council adjustments to the plan in the light of changes in the telecommunication/ICT environment and/or as a result of the performance evaluation and the risk management framework, in particular by:

i) making all modifications necessary to ensure that the strategic plan facilitates the accomplishment of ITU's goals and objectives, taking account of proposals by the Sector advisory groups, decisions by conferences and by assemblies of the Sectors and changes in the strategic focus of the Union's activities, within the financial limits established by the Plenipotentiary Conference;

ii) ensuring the linkage between the strategic, financial and operational plans in ITU, and developing the corresponding human resources strategic plan,

instructs the Council

1 to oversee further development of the ITU results framework, including the adoption of the related indicators that will enable to better measure the effectiveness and efficiency of the implementation of the strategic plan of the Union (Annex 1);

2 to monitor the implementation of the strategic plan of the Union in Annex 1 to this resolution, and when necessary adjust the strategic plan, on the basis of the Secretary-General's reports;

3 to present an assessment of the results of the strategic plan for 2020-2023 to the next plenipotentiary conference, along with a proposed strategic plan for the period 2024-2027;

4 to ensure that the rolling operational plans from the General Secretariat and the three Sectors approved annually by Council are fully aligned and compliant with this Resolution and its annexes and with the Financial Plan for the Union approved in Decision 5 of this Conference,

invites the Member States

to contribute national and regional insights on policy, regulatory and operational matters to the strategic planning process undertaken by the Union in the period before the next plenipotentiary conference, in order to:

− strengthen the effectiveness of the Union in fulfilling its purposes as set out in the instruments of the Union, by cooperating in the implementation of the strategic plan;

− assist the Union in meeting the changing expectations of all its constituents as national structures for the provision of telecommunication/ICT services continue to evolve,

invites Sector Members

to communicate their views on the strategic plan of the Union through their relevant Sectors and the corresponding advisory groups.

**Reasons:** Brazil proposes amendments in the body of Resolution 71 (not including the Annexes) to reinforce the concept of "ONE ITU" by strengthening the activities of the regional offices in the areas of standardization and radiocommunications, and by enhancing the mechanisms for monitoring and controlling the elaboration and implementation of sectoral operational plans.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

SUP B/67/3

RESOLUTION 128 (Rev. Antalya, 2006)

Support for the Agenda for Connectivity in the Americas and Quito Action Plan

The Plenipotentiary Conference of the International Telecommunication Union (Antalya, 2006),

**Reasons:** Brazil proposes suppression of resolution 128 due to the non-relevance of the "Connectivity Agenda of the Americas" and the "Plan of Action of Quito" in the current telecommunication/ICT environment, and the suppression of Resolution 39 by the World Telecommunication Development Conference 2017 (WTDC-17) on the same subject.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

MOD B/67/4

RESOLUTION 130 (Rev. Dubai, 2018)

Strengthening the role of ITU in Cybersecurity

The Plenipotentiary Conference of the International Telecommunication Union (Dubai, 2018),

recalling

*a)* United Nations General Assembly (UNGA) Resolution 68/198, on information and communication technologies (ICTs) for development;

*b)* UNGA Resolution 68/167, on the right to privacy in the digital age;

*c)* UNGA Resolution 68/243, on developments in the field of information and telecommunications in the context of international security;

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

*e)* UNGA Resolution 70/125, on the outcome document of the high-level meeting of the General Assembly on the overall review of the implementation outcomes of the WSIS;

*f)* Resolution 174 (Rev. Busan, 2014) of this conference;

*g)* Resolution 181 (Rev. Guadalajara, 2010) of the Plenipotentiary Conference;

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

*i)* Resolution 140 (Rev. Busan, 2014) of this conference;

*j)* Resolution 69 (Rev. Buenos Aires, 2017) of WTDC, on facilitating creation of national computer incident response teams, particularly for developing countries[[1]](#footnote-1)1, and cooperation between them;

*k)* that ITU Council Resolution 1305, adopted at its 2009 session, identified the security, safety, continuity, sustainability and robustness of the Internet as public policy issues that fall within the scope of ITU,

considering

*a)* that UNGA Resolution 70/125, which represents the Outcome document of the high-level meeting of the General Assembly on the overall review of the implementation outcomes of the WSIS, affirms that “*the same rights that people have offline must also be protected online. We emphasize that progress towards the vision of the World Summit on the Information Society should be considered not only as a function of economic development and the spreading of information and communications technologies but also as a function of progress with respect to the realization of human rights and fundamental freedoms” and that “building confidence and security in the use of information and communications technologies for sustainable development should also be a priority, especially given growing challenges, including the abuse of such technologies for harmful activities from harassment to crime to terrorism*”;

*b)* that, with the application and development of ICTs, new threats from various sources have emerged, that have had an impact on confidence and security in the use of ICTs by all Member States, Sector Members and other stakeholders, including all users of ICTs, and on the preservation of peace and the economic and social development of all Member States, and that threats to and vulnerabilities of infrastructure and networks continue to give rise to ever-growing security challenges across national borders for all countries;

*c)* that the ITU signed a cooperation agreement with the Forum for Incident Response and Security Teams (FIRST) to collaborate within the framework of the ITU Global Cybersecurity Agenda and to facilitate the affiliation process of ITU Member States’ national CIRTs to FIRST;

*d)* the ITU Global Cybersecurity Agenda (GCA), which encourages international cooperation aimed at proposing strategies for solutions to enhance confidence and security in the use of telecommunications/ICTs;

*e)* that, in order to protect these infrastructures and address these challenges and threats, coordinated national, regional and international action is required for prevention, preparation, response and recovery from computer security incidents, on the part of government authorities, at the national (including the creation of national computer incident response teams (CIRTs)), and sub-national levels, the private sector and citizens and users, in addition to international and regional cooperation and coordination, and that ITU has a lead role to play within its mandate and competencies in this field;

*f)* the need for continual evolution in new technologies to support the early detection of, and coordinated and timely response to, events or incidents compromising computer security, or computer network security incidents that could compromise the availability, integrity and confidentiality of critical infrastructures in ITU Member States, and for strategies that will minimize the impact of such incidents and mitigate the growing risks and threats to which such platforms are exposed;

*g)* that the ITU Telecommunication Standardization Sector (ITU‑T) has adopted around 300 standards relating to building confidence and security in the use of ICTs;

*h)* the final report on Question 22‑1/1 (Securing information and communication networks: Best practices for developing a culture of cybersecurity) of the ITU Telecommunication Development Sector (ITU‑D);

*i)* that some SMEs face additional challenges at ensuring cybersecurity at implementing instrumental practices such as patching IT systems, updating operating systems, implementing preventive, response and recovery plans, complying with government and industry norms and regulations and fostering continuous capacity building;

*j)* that the technical community and the private sector are key players in the development and deployment of new technologies and their applications should incorporate holistic approaches in which cybersecurity is seen as a continuous process;

*k)* that individuals and organisations should adopt best practices that allow for flexible risk-based and consensus-based approaches, available technical safeguards as part of informed and responsible user behaviour, and that greater capacity building and awareness-raising efforts are required in this regard,

recognizing

*a)* that the development of ICTs has been and continues to be instrumental for the growth and development of the global economy, underpinned by security and trust;

*b)* that the World Summit on the Information Society (WSIS) affirmed the importance of building confidence and security in the use of ICTs and the great importance of multistakeholder implementation at the international level, and established Action Line C5 (Building confidence and security in the use of ICTs), with ITU identified in the Tunis Agenda for the Information Society as moderator/facilitator for the action line, and that this task has been carried out by the Union in recent years, for example under GCA;

*c)* that WTDC‑14 has adopted Resolution 45 (Rev. Dubai, 2014), on mechanisms for enhancing cooperation on cybersecurity, including countering and combating spam, calling on the Secretary-General to bring the resolution to the attention of the next plenipotentiary conference for consideration and required action, and to report the results of these main areas of work to the Council and to the Plenipotentiary Conference in 2018, as appropriate; and WTDC-17 has adopted the Buenos Aires Action Plan, which identifies cybersecurity as a priority in Objective 2, and Resolution 69 (Rev. Buenos Aires, 2017), on facilitating creation of national CIRTs, particularly for developing countries, and cooperation between them;

*d)* that, to support the creation of national CIRTs in Member States where these are needed and are currently absent, the World Telecommunication Standardization Assembly (WTSA) adopted Resolution 58 (Rev. Hammamet, 2016), on encouraging the creation of national CIRTs, particularly for developing countries; and WTDC‑17 adopted Resolution 69 (Rev. Buenos Aires, 2017), on facilitating creation of national CIRTs, including CIRTs responsible for government-to-government cooperation, particularly for developing countries, cooperation among them, and the importance of coordination among all relevant organizations;

*e)* § 15 of the Tunis Commitment, which states: "*Recognizing the principles of universal and non-discriminatory access to ICTs for all nations, the need to take into account the level of social and economic development of each country, and respecting the development-oriented aspects of the information society, we underscore that ICTs are effective tools to promote peace, security and stability, to enhance democracy, social cohesion, good governance and the rule of law, at national, regional and international levels. ICTs can be used to promote economic growth and enterprise development. Infrastructure development, human capacity building, information security and network security are critical to achieve these goals. We further recognize the need to effectively confront challenges and threats resulting from use of ICTs for purposes that are inconsistent with objectives of maintaining international stability and security and may adversely affect the integrity of the infrastructure within States, to the detriment of their security. It is necessary to prevent the abuse of information resources and technologies for criminal and terrorist purposes, while respecting human rights*";

*f)* that the ITU‑coordinated WSIS+10 High-Level Event identified several challenges in the implementation of the WSIS action lines that still remain and that will need to be addressed beyond 2015;

*g)* that Member States, in particular developing countries, in the elaboration of appropriate and workable legal measures relating to protection against cyberthreats at the national, regional and international levels, may require assistance from ITU in establishing technical and procedural measures, aimed at securing national ICT infrastructures, on request from these Member States, while noting that there are a number of regional and international initiatives which may support these countries in elaborating such legal measures;

*h)* Opinion 4 (Lisbon, 2009) of the World Telecommunication/ICT Policy Forum, on collaborative strategies for creating confidence and security in the use of ICTs;

*i*) Resolution 50 (Rev. Hammamet, 2016), on cybersecurity, that resolves to continue to give cybersecurity 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;

*j)* that the development of human skills and capacity building are key to enhance the protection of information networks;

*k)* that Member states are constantly making efforts to improve institutional environments;

*l)* That cyber-risk assessment or cyber risk cost analysis and the calculation of risk exposure provide a better evaluation of the enterprise cyber-hygiene and its risk position,

aware

*a)* that ITU and other international organizations, through a variety of activities, are examining issues related to building confidence and security in the use of ICTs, including stability and measures to combat spam, malware, etc., and to protect personal data and privacy;

*b)* of the negative impact that unauthorized surveillance and/or interception of communications as well as the collection of data, in particular when carried out on a mass scale, have on the exercise and enjoyment of human rights;

*c)* that ITU‑T Study Group 17, ITU-D Study Groups 1 and 2 and other relevant ITU study groups continue to work on technical means for the security of information and communication networks, in accordance with Resolutions 50 and 52 (Rev. Hammamet, 2016) of WTSA and Resolutions 45 (Rev. Dubai, 2014) and 69 (Rev. Buenos Aires, 2017) of WTDC;

*d)* that ITU has a fundamental role to play in building confidence and security in the use of ICTs;

*e)* that ITU‑D Study Group 2 continues to carry out the studies called for in ITU‑D Question 3/2 (Securing information and communications networks: Best practices for developing a culture of cybersecurity), which has been reflected in UNGA Resolution 64/211;

*f)* that ITU is also assisting developing countries in building confidence and security in the use of ICTs and supporting the establishment of CIRTs, including CIRTs responsible for government-to-government cooperation, and the importance of coordination among all relevant organizations;

*g)* that Council Resolution 1336, adopted at its 2011 session, established a working group of the Council on international Internet-related public policy issues (CWG-Internet), whose terms of reference are to identify, study and develop matters related to international Internet-related public policy issues, including those issues identified in Council Resolution 1305 (2009) such as security safety, continuity, sustainability and robustness of the Internet;

*h)* that WTDC‑17 adopted Resolution 80 (Rev. Buenos Aires, 2017), on establishing and promoting trusted information frameworks in developing countries to facilitate and encourage electronic exchanges of economic information between economic partners;

*i)* of Article 6, on security and robustness of networks, and Article 7, on unsolicited bulk electronic communications, of the International Telecommunication Regulations adopted by the World Conference on International Telecommunications (Dubai, 2012),

noting

*a)* that, as an intergovernmental organization with private‑sector participation, ITU is well-positioned to play an important role, together with other relevant international bodies and organizations, in addressing threats and vulnerabilities, which affect efforts to build confidence and security in the use of ICTs;

*b)* §§ 35 and 36 of the Geneva Declaration of Principles and § 39 of the Tunis Agenda, on building confidence and security in the use of ICTs;

*c)* that although there are no universally agreed upon definitions of spam and other terms in this sphere, spam was characterized by ITU‑T Study Group 2, at its June 2006 session, as a term commonly used to describe unsolicited electronic bulk communications over e‑mail or mobile messaging (SMS, MMS), usually with the objective of marketing commercial products or services,

resolves

1 to continue to give this work high priority within ITU, in accordance with its competences and expertise, including promoting common understanding among governments and other stakeholders of building confidence and security in the use of ICTs at national, regional and international level;

2 to give high priority to the work of ITU, in accordance with its competencies and areas of expertise, and to continue to work closely, as appropriate, with other relevant bodies/agencies within the United Nations and other relevant international bodies, taking into account the specific mandates and areas of expertise of the different agencies, while being mindful of the need to avoid duplicating work between organizations and among the Bureaux or the General Secretariat;

3 that ITU shall focus resources and programmes on those areas of cybersecurity within its core mandate and expertise, notably the technical and development spheres, and not including areas related to Member States' application of legal or policy principles related to national defence, national security, content and cybercrime, which are within their sovereign rights, although this does not however exclude ITU from carrying out its mandate to develop technical recommendations designed to reduce vulnerabilities in the ICT infrastructure, nor from providing all the assistance that was agreed upon at WTDC‑14 (Resolution 45) and WTDC-17, including Objective 2 and in activities under Question 3/2;

4 to contribute to further strengthening the trust and security framework, consistent with ITU's role as lead facilitator of WSIS Action Line C5, taking into account Resolution 140 (Rev. Busan, 2014);

5 to respect and protect telecommunication/ICT related aspects of data protection as a principle to further strengthen cybersecurity, within ITU’s core mandate and expertise;

6 to study the specific cybersecurity challenges faced by SMEs, especially their resource limitation, and the best practices, initiatives and guidelines designed to overcome them;

7 to provide membership with an assessment of the positive and negative impacts of the deployment of emerging technologies in the field of cybersecurity, including the need to take measures to put an end to violations of those rights and to create the conditions to prevent such violations, including by ensuring that relevant national legislation complies with their obligations under international human rights law;

8 To promote a study of institutional approaches related to cybersecurity issues in cooperation with member states and other international organizations,

instructs the Secretary-General and the Directors of the Bureaux

1 to continue to review:

i) the work done so far in the three Sectors, under the ITU Global Cybersecurity Agenda and in other relevant organizations and initiatives to address existing and future threats in order to build confidence and security in the use of ICTs;

ii) the progress achieved in the implementation of this resolution, with ITU continuing to play a lead facilitating role as the moderator/facilitator for Action Line C5, with the help of the advisory groups, consistent with the ITU Constitution and the ITU Convention;

2 consistent with Resolution 45 (Rev. Dubai, 2014), to report to the Council on activities within ITU and other relevant organizations and entities to enhance cooperation and collaboration, regionally and globally, to strengthen building confidence and security in the use of ICTs of Member States, in particular developing countries, taking into account any information provided by Member States, including information on situations within their own jurisdiction that could affect this cooperation;

3 consistent with Resolution 45 (Rev. Dubai, 2014), to report on memoranda of understanding (MoU) between countries, as well as existing forms of cooperation, providing analysis of their status, scope and how these cooperative mechanisms can be applied to strengthen cybersecurity and combat cyberthreats, with a view to enabling Member States to identify whether additional memoranda or mechanisms are required;

4 to facilitate access to tools and resources, within the available budget, required for enhancing confidence and security in the use of ICTs for all Member States, consistent with WSIS provisions on universal and non-discriminatory access to ICTs for all nations;

5 to continue to maintain the cybersecurity gateway as a way to share information on national, regional and international cybersecurity-related initiatives worldwide;

6 to report annually to the Council on these activities and to make proposals as appropriate;

7 to further enhance coordination between the study groups and programmes concerned,

instructs the Director of the Telecommunication Standardization Bureau

1 to intensify work within existing ITU‑T study groups in order to:

i) address existing and future threats and vulnerabilities affecting efforts to build confidence and security in the use of ICTs, by developing reports or recommendations, as appropriate, with the goal of implementing the resolutions of WTSA‑16, particularly Resolutions 50 and 52 (Rev. Hammamet, 2016) and 58 (Rev. Dubai, 2012), allowing work to begin before a question is approved;

ii) seek ways to enhance the exchange of technical information in these fields, promote the adoption of protocols and standards that enhance security, and promote international cooperation among appropriate entities;

iii) facilitate projects deriving from the outcomes of WTSA‑12, in particular:

• Resolution 50 (Rev. Hammamet, 2016), on cybersecurity;

• Resolution 52 (Rev. Hammamet, 2016), on countering and combating spam;

2 to continue collaboration with relevant organizations with a view to exchanging best practices and disseminating information through, for example, joint workshops and training sessions and joint coordination activity groups, and, by invitation, through written contributions from relevant organizations,

instructs the Director of the Telecommunication Development Bureau

1 consistent with the results of WTDC‑14 and pursuant to Resolutions 45 (Rev. Dubai, 2014), Resolutions 69 and 80 (Rev. Buenos Aires, 2017) and Objective 2 of the Buenos Aires Action Plan, to support ongoing regional and global cybersecurity projects, and to encourage all countries to take part in these activities;

2 upon request, to support ITU Member States in their efforts to build capacity, by facilitating Member States' access to resources developed by other relevant international organizations that are working on national legislation to combat cybercrime; supporting ITU Member States' national and regional efforts to build capacity to protect against cyberthreats/cybercrime, in collaboration with one another; consistent with the national legislation of Member States referred to above, assisting Member States, in particular developing countries, in the elaboration of appropriate and workable legal measures relating to protection against cyberthreats at national, regional and international levels; establishing technical and procedural measures, aimed at securing national ICT infrastructures, taking into the account the work of the relevant ITU‑T study groups and, as appropriate, other relevant organizations; establishing organizational structures, such as CIRTs, to identify, manage and respond to cyberthreats, and cooperation mechanisms at the regional and international level;

3 to provide the necessary financial and administrative support for these projects within existing resources, and to seek additional resources (in cash and in kind) for the implementation of these projects through partnership agreements;

4 to ensure coordination of the work of these projects within the context of ITU's overall activities in its role as moderator/facilitator for WSIS Action Line C5, and to eliminate any duplication regarding this important subject with the General Secretariat and ITU‑T;

5 to coordinate the work of these projects with that of the ITU‑D study groups on this topic, and with the relevant programme activities and the General Secretariat;

6 to continue collaboration with relevant organizations with a view to exchanging best practices and disseminating information through, for example, joint workshops and training sessions;

7 to support ITU Member States in the development of their national and/or regional cybersecurity strategies toward building national capabilities for dealing with cyberthreats in accordance with the principles of international cooperation, consistent with Objective 3 of the Buenos Aires Action Plan;

8 to support the membership in the development of human skills and capacity building to enhance cybersecurity;

9 to support the membership in the risk assessment activities related to cybersecurity;

10 to report annually to the Council on these activities and make proposals as appropriate,

further instructs the Director of the Telecommunication Standardization Bureau and the Director of the Telecommunication Development Bureau

each within the scope of their responsibilities:

1 to implement relevant resolutions of both WTSA‑16 and WTDC‑17, including the programme described in Objective 2 of the Buenos Aires Action Plan, on providing support and assistance to developing countries in building confidence and security in the use of ICTs;

2 to identify and promote the availability of information on building confidence and security in the use of ICTs, specifically related to the ICT infrastructure, for Member States, Sector Members and relevant organizations;

3 without duplicating the work under ITU‑D Question 3/2, to identify best practices in establishing CIRTs, to prepare a reference guide for the Member States and, where appropriate, to contribute to Question 3/2;

4 to cooperate with relevant organizations and other relevant international and national experts, as appropriate, in order to identify best practices in the establishment of CIRTs;

5 to take action with a view to new questions being examined by the study groups within the Sectors on the establishment of confidence and security in the use of ICTs;

6 to identify and document practical steps to strengthen security in the use of ICTs internationally, based on widely accepted practices, guidelines and recommendations that Member States can choose to apply to improve their ability to combat cyberthreats and attacks and to strengthen international cooperation in building confidence and security in the use of ICTs, taking into account the ITU Global Cybersecurity Agenda (GCA) and within the available financial resources;

7 to support strategy, organization, awareness-raising, cooperation, evaluation and skills development;

8 to provide the necessary technical and financial support, within the constraints of existing budgetary resources, in accordance with Resolution 58 (Rev. Dubai, 2012);

9 to encourage the study of security threats and vulnerabilities in conjunction with experts and the membership;

10 to foster the discussion of the concept of security by design and its possible application in the technical recommendations, as well as in guidelines for regulatory policies to the benefit of its Membership;

11 to study the effects of cybersecurity on socioeconomic development and to develop metrics to measure the outcomes of the investment in this field;

12 to mobilize appropriate extrabudgetary resources, outside the regular budget of the Union, for the implementation of this resolution, to help developing countries,

instructs the Secretary-General

pursuant to his initiative on this matter:

1 to report to the Council, taking into account the activities of the three Sectors, on the implementation and effectiveness of the action plan to strengthen the role of ITU in building confidence and security in the use of ICTs;

2 to cooperate with relevant international organizations, including through the adoption of MoUs, subject to the approval of the Council in this regard, in accordance with Resolution 100 (Minneapolis, 1998) of the Plenipotentiary Conference,

requests the Council

to include the report of the Secretary-General in the documents sent to Member States in accordance with No. 81 of the Convention,

invites Member States

1 to consider joining appropriate competent international and regional initiatives for enhancing national legislative frameworks relevant to the security of information and communication networks;

2 to closely collaborate in strengthening regional and international cooperation, taking into account Resolution 45 (Rev. Dubai, 2014), with a view to enhancing confidence and security in the use of ICTs, in order to mitigate risks and threats;

3 to support ITU initiatives on cybersecurity, including the Global Cybersecurity Index (GCI), in order to promote government strategies and the sharing of information on efforts across industries and sectors;

4 to inform the Secretary-General of relevant activities related to this resolution regarding confidence and security in the use of ICTs,

invites Member States, Sector Members and Associates

1 to contribute on this subject to the relevant ITU study groups and to any other activities for which the Union is responsible;

2 to contribute to building confidence and security in the use of ICTs at the national, regional and international levels, by undertaking activities as outlined in § 12 of the Geneva Plan of Action, and to contribute to the preparation of studies in these areas;

3 to promote the development of educational and training programmes to enhance user awareness of risks in cyberspace;

4 to collaborate, as appropriate, in order to address and prevent problems that undermine confidence and security in the use of telecommunications/ICTs.

**Reasons:** The Brazilian proposal drives the ITU to discuss specific challenges that small and medium-sized enterprises face in cybersecurity and to elaborate best practices; emphasizes the importance of disseminating and promoting best practices and training in cybersecurity among individuals and organizations; promotes risk and cost-benefit analysis in the assessment of institutional exposure to cyber security threats; points out the need to prevent and remedy breaches of privacy and human rights resulting from unauthorized interception of communications; promotes the importance of data protection as a key element in cybersecurity; and instructs the ITU to discuss the definition and use of the concept of “security by design” in the ITU technical recommendations.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

ADD B/67/5

Draft New Resolution [B-1]

International public policy issues concerning telecommunications-related aspects of OTT applications

The Plenipotentiary Conference of the International Telecommunication Union (Dubai, 2018),

recalling

*a)* the principles on Internet-related policymaking set out in

• the outcomes of the World Summit on the Information Society (WSIS) and the WSIS+10 High-Level meetings;

• United Nations General Assembly Resolution A/RES/70/125 that adopted 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;

*b)* the ITU’s core purposes as defined in the ITU Constitution;

*c)* ITU Resolutions 102 (Rev. Dubai, 2018) and 140 (Rev. Dubai, 2018), particularly the provisions related to the role of the ITU and governments in Internet-related policymaking, in consultation with all relevant stakeholders;

*d)* the outcomes of the Tunis Agenda (paras. 35, 36, 67), such as the multi-stakeholder policy dialogue and the complexity of the ecosystem translated by the many different forums conceived for Internet policy discussions;

*e)* the importance of the Internet Governance Forum for Internet-related policy discussions (Tunis Agenda, paras 72 and 73);

*f)* the debates on OTT carried out in other relevant organizations, including standards development organizations (SDO) and policy development organizations,

considering

*a)* that paragraph 15 of the 2030 Agenda for Sustainable Development highlights the great potential of ICTs and global interconnectedness to accelerate human progress, bridge the digital divide and develop knowledge societies, thus contributing to achieving and accelerating the achievement of the Sustainable Development Goals;

*b)* that Over the Top (OTT) applications enable governments, businesses and individuals to benefit, participate and contribute actively to the digital economy and to sustainable socioeconomic development;

*c)* that the inherent cross-border nature of OTTs requires collaboration and coordination between governments and all stakeholders at the international level,

recognizing

*a)* the fundamental differences between traditional telecommunications services and OTTs, including inter alia, control of broadband infrastructure, level of regulatory exposure, barriers to entry, competitive environment and interconnection to public networks;

*b)* that network operators and OTT are part of the same ecosystem, which implies important inter-dependencies between them;

*c)* that the relationship between OTTs and traditional telecommunications services can be leveraged to expand connectivity to unserved and underserved populations;

*e)* that the mutual cooperation between OTTs and telecommunication operators can be an element to foster innovative, sustainable, viable business models and their positive roles in fostering socioeconomic benefits;

*f)* that the expansion of OTTs sets technical, economic, social and policy challenges and opportunities for governments and the telecommunication/ICTs industry,

recognizing further

*а)* studies by Study Group 3 and Study Group 17 of ITU-T, in particular the approval of a definition for OTTs in the scope of the ITU by ITU-T Recommendation D.262 and ITU-T Study Group 3 Technical Report “Economic Impact of OTTs” (2017);

*b)* studies by Study Group 1 of ITU-D, and the approval by the 2017 World Telecommunication Development Conference of Study Question 3/1 on “Emerging technologies, including cloud computing, m-services and OTTs: Challenges and opportunities, economic and policy impact for developing countries;”

*с)* inputs of stakeholders presented to the 5th Open Consultation of CWG-Internet on "Public Policy Considerations for OTT," and the discussions held at the physical open consultation meeting on September 18, 2017;

*d)* The Final Report of the 10th meeting of CWG-Internet, which demonstrates a wide variety of perspectives from Member States on the appropriate role of the ITU with respect to OTTs,

resolves

1 to raise awareness and promote a common understanding among the membership of an enabling environment for telecommunication-related aspects of OTT applications within the ITU;

2 to foster technical, economic and policy studies in telecommunication-related aspects of OTT applications within the ITU,

instructs the Sector Advisory Groups

to identify and foster the study of issues associated with telecommunication-related aspects of OTT applications in the Sectors’ Study Groups, in accordance with their expertise and purpose,

instructs CWG-Internet

to submit an annual report to Council on the activities undertaken on telecommunication-related aspects of OTT applications in the ITU, consistent with the work of ITU Study Groups and Advisory Groups, contributions from Member States and Sector Members and open consultation materials,

instructs the Directors of the Bureaux

to collaborate closely with the CWG-Internet and the Sector Advisory Groups to provide information on the matters of this Resolution,

invites Member States and Sector Members

to contribute to the above activities and take active part in the implementation of this Resolution.

**Reasons:** Some Over-The-Top (OTT) applications (henceforth “OTTs”) have been enhancing and gradually substituting traditional telecommunication/ICTs for the past 20 years. The correlation and interdependence between telecommunication/ICTs and OTTs has increasingly driven ITU to debate issues related to OTTs.

In September 2017, the ITU Council Working Group on international Internet-related public policy issues (CWG-Internet) conducted its 5th open physical consultation on “Policy considerations related to OTTs.” It was a successful consultation, with 70 contributions from all types of stakeholders and all regions, and extensive debate in the physical consultation and in CWG-Internet.

Brazilian stakeholders submitted eight contributions to the public consultation. The Brazilian administration presented a contribution to CWG-Internet explaining the multi-stakeholder framework for discussion of OTT issues in Brazil, listing the issues relevant to the OTT ecosystem, proposing that discussions on OTTs in ITU focus on telecommunication-related OTTs, and asking that the multi-stakeholder Internet governance principles established by the World Summit on the Information Society (WSIS) be observed[[2]](#footnote-2).

WTDC-17 approved the creation in ITU-D of Question 3/1 on “Emerging technologies, including cloud computing: m-services, and OTTs: Challenges and opportunities, economic and policy impact for developing countries.” Study Group 3 of the ITU-T approved in April 2018 Draft Recommendation ITU-T D.262 “Collaborative Framework for OTTs” that defines OTT as

*“An application accessed and delivered over the public Internet that may be a direct technical / functional substitute for traditional international telecommunications services. (NOTE – The definition of OTT is a matter of national sovereignty and may vary among Member States).”* [[3]](#footnote-3)

Thus, Brazil sees with satisfaction the level of attention attributed to OTTs by the ITU Council, by the 2017 World Telecommunication Development Conference (WTDC-17) and by Study Group 3 of the ITU-T.

Both in ITU-T and ITU-D, discussions will involve ITU Sector Members, which include OTT providers, telecommunication operators, civil society and academic institutions, the technical community and other international organizations.

Much has been achieved in the ITU in issues surrounding OTTs. The draft new Resolution in Annex I aims to recognize and enhance the work that is being carried out currently in the ITU, to foster improved follow-up and monitoring of issues of telecommunication-related aspects of OTT applications that can be a direct technical / functional substitute for traditional international telecommunications services in all instances of the ITU, and to ensure the observation of the multi-stakeholder Internet governance principles established by WSIS.

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

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. <https://www.itu.int/md/S17-RCLINTPOL10-C-0005/en> [↑](#footnote-ref-2)
3. <https://www.itu.int/md/T17-SG03-R-0011/en> [↑](#footnote-ref-3)