|  |  |
| --- | --- |
| **Plenipotentiary Conference (PP-18) Dubai, 29 October – 16 November 2018** |  |
|  |  |
|  |  |
| WORKING GROUP OF THE PLENARY | **Document DL/5-E** |
|  | **30 October 2018** |
|  | **English only** |
|  | |
| AD-Hoc Group on Res 130, 174 and new proposed Res. on Data protection  (Cybersecurity related issues) | |
| Consolidated Text Resolution 130 | |
|  | |
|  | |

RESOLUTION 130 (Rev. dUBAI, 2018)

Strengthening the role of ITU in building confidence and security in the use of information and communication technologies

|  |
| --- |
| **B/67/4 : Brazil**  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;

|  |
| --- |
| **IAP/63A1/35 : Inter-American Proposals**  *d)* UNGA Resolution 64/211, on the Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures; |

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

|  |
| --- |
| **IAP/63A1/35 : Inter-American Proposals**  *e)* UNGA Resolution 57/239, on the creation of a global culture of cybersecurity; |

|  |
| --- |
| **ARB/72A1/11 : Arab States Common Proposals**  *e)* UNGA Resolution 70/125, the outcome document of the high-level meeting of the General Assembly on the overall review of the implementation of WSIS outcomes; |

*e)* the outcome documents of the WSIS+10 High-Level Event, containing the WSIS+10 Statement on the Implementation of WSIS Outcomes and the WSIS+10 Vision for WSIS Beyond 2015;

|  |
| --- |
| **EUR/48A1/2 : European Common Proposals**  *e)* UNGA Resolution 70/125, the outcome document of the high-level meeting of the General Assembly on the overall review of the implementation of WSIS outcomes; |

|  |
| --- |
| **IAP/63A1/35 : Inter-American Proposals**  *f)* UNGA Resolution 70/125, 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; |

|  |
| --- |
| **ARB/72A1/11 : Arab States Common Proposals**  *f)* the outcome documents of the WSIS+10 High-Level Event, containing the WSIS+10 Statement on the Implementation of WSIS Outcomes and the WSIS+10 Vision for WSIS Beyond 2015; |

|  |
| --- |
| **B/67/4 : Brazil**  *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;

|  |
| --- |
| **IAP/63A1/35 : Inter-American Proposals**  *g)* Resolution 174 (Rev. Busan, 2014) of this conference on the ITU's role with regard to international public policy issues relating to the risk of illicit use of information and communication technologies; |

|  |
| --- |
| **ARB/72A1/11 : Arab States Common Proposals**  *g)* Resolution 174 (Rev. Busan, 2014) of this conference; |

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

|  |
| --- |
| **EUR/48A1/2 : European Common Proposals**  *g)* Resolution 181 (Guadalajara, 2010) of the Plenipotentiary Conference; |

|  |
| --- |
| **IAP/63A1/35 : Inter-American Proposals**  *h)* Resolution 181 (Guadalajara, 2010) of the Plenipotentiary Conference on the Definitions and terminology relating to building confidence and security in the use of information and communication technologies; |

|  |
| --- |
| **ARB/72A1/11 : Arab States Common Proposals**  *h)* 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;

|  |
| --- |
| **EUR/48A1/2 : European Common Proposals** |

|  |
| --- |
| **IAP/63A1/35 : Inter-American Proposals**  *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; |

|  |
| --- |
| **ARB/72A1/11 : Arab States Common Proposals**  *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; |

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

|  |
| --- |
| **EUR/48A1/2 : European Common Proposals** |

|  |
| --- |
| **IAP/63A1/35 : Inter-American Proposals**  *j)* Resolution 140 (Rev. Busan, 2014) of this conference ITU's role in implementing the outcomes of the World Summit on the Information Society and in the overall review by United Nations General Assembly of their implementation; |

|  |
| --- |
| **ARB/72A1/11 : Arab States Common Proposals**  *j)* Resolution 140 (Rev. Busan, 2014) of this conference; |

*j)* Resolution 69 (Rev. Dubai, 2014) of WTDC, on the creation of national computer incident response teams (CIRTs), particularly for developing countries1, and cooperation between them;

|  |
| --- |
| **[[1]](#footnote-1)EUR/48A1/2 : European Common Proposals** |

|  |
| --- |
| **AFCP/55A1/3 : African Common Proposals**  *j)* Resolution 69 (Rev. Buenos Aires, 2017) of WTDC, on the creation of national computer incident response teams (CIRTs), particularly for developing countries1, and cooperation between them; |

|  |
| --- |
| **[[2]](#footnote-3)IAP/63A1/35 : Inter-American Proposals**  *k)* Resolution 69 (Rev. Buenos Aires, 2017) of WTDC, on the creation of national computer incident response teams (CIRTs), particularly for developing countries1, and cooperation between them; |

|  |
| --- |
| **[[3]](#footnote-4)ACP/64A1/13 : Asia-Pacific Common Proposals**  *j)* Resolution 69 (Rev. Buenos Aires, 2017) of WTDC, on facilitating creation of national computer incident response teams (CIRTs), particularly for developing countries1, and cooperation between them;  *[[4]](#footnote-5)k)* Resolution 179 (Rev. Busan, 2014) on ITU's role in child online protection and Resolution 67 (Rev. Buenos Aires, 2017) of WTDC on the role of the ITU Telecommunication Development Sector (ITU‑D) in child online protection; |

|  |
| --- |
| **ARB/72A1/11 : Arab States Common Proposals**  *k)* Resolution 69 (Rev. Dubai, 2014) of WTDC, on the creation of national computer incident response teams (CIRTs), particularly for developing countries1, and cooperation between them; |

|  |
| --- |
| **[[5]](#footnote-6)B/67/4 : Brazil**  *j)* Resolution 69 (Rev. Buenos Aires, 2017) of WTDC, on facilitating creation of national computer incident response teams, particularly for developing countries1, and cooperation between them; |

*[[6]](#footnote-7)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,

|  |
| --- |
| **EUR/48A1/2 : European Common Proposals**  *h)* Resolution 140 (Rev. Busan, 2014) of this conference, |

|  |
| --- |
| **IAP/63A1/35 : Inter-American Proposals**  *l)* 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,  *m)* Resolution 58 (Rev. Dubai, 2012) of the WTSA on the Encouraging the creation of national computer incident response teams, particularly for developing countries |

|  |
| --- |
| **ACP/64A1/13 : Asia-Pacific Common Proposals**  *l)* 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, |

|  |
| --- |
| **ARB/72A1/11 : Arab States Common Proposals**  *l)* 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;  *m)* the cybersecurity-related provisions of the Tunis Commitment and the Tunis Agenda and the outcome document of the HLM of the UNGA on the overall review of the implementation of WSIS, |

considering

|  |
| --- |
| **ARB/72A1/11 : Arab States Common Proposals**  *a)* that ICTs has become essential to our daily lives, as it promotes social, cultural and economic growth and development of local communities in various ways, and has numerous implications for the interaction of individuals with their local communities and with the wider world;  *b)* Resolution 179 (Rev. Busan, 2014) of this conference, on ITU's role in child online protection and Resolution 67 (Rev. Buenos Aires, 2017) of WTDC, on the role of the ITU Telecommunication Development Sector (ITU D) in child online protection; |

*a)* that the ITU‑coordinated WSIS+10 High-Level Event reaffirmed the importance of building confidence and security in the use of ICTs, as mentioned in relevant paragraphs of the WSIS+10 outcome documents (Geneva, 2014);

|  |
| --- |
| **EUR/48A1/2 : European Common Proposals**  *a)* that UNGA Resolution 70/125, the outcome document of the high-level meeting of the General Assembly on the overall review of the implementation of WSIS outcomes, affirmed that strengthening confidence and security in the use of information and communications technologies for the development of information societies and the success of such technologies is a driver for economic and social innovation ; |

|  |
| --- |
| **IAP/63A1/35 : Inter-American Proposals** |

|  |
| --- |
| **ARB/72A1/11 : Arab States Common Proposals**  *c)* that the ITU‑coordinated WSIS+10 High-Level Event reaffirmed the importance of building confidence and security in the use of ICTs, as mentioned in relevant paragraphs of the WSIS+10 outcome documents (Geneva, 2014); |

|  |
| --- |
| **B/67/4 : Brazil** |

*b)* the crucial importance of information and communication infrastructures and their applications to practically all forms of social and economic activity;

|  |
| --- |
| **EUR/48A1/2 : European Common Proposals**  *b)* the crucial importance of information and communication technology to practically all forms of social and economic activity; |

|  |
| --- |
| **IAP/63A1/35 : Inter-American Proposals** |

|  |
| --- |
| **ARB/72A1/11 : Arab States Common Proposals**  *d)* the crucial importance of information and communication infrastructures and their applications to practically all forms of social and economic activity; |

|  |
| --- |
| **B/67/4 : Brazil**  *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*”; |

*c)* 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 networks continue to give rise to ever-growing security challenges across national borders for all countries, in particular developing countries, while noting in this context the strengthening of ITU's role in building confidence and security in the use of ICTs and the need to further enhance international cooperation and develop appropriate existing national, regional and international mechanisms (for example, agreements, best practices, memoranda of understanding, etc.);

|  |
| --- |
| **EUR/48A1/2 : European Common Proposals**  *c)* 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 economic and social development of all Member States, and that threats to and vulnerabilities of networks and devices continue to give rise to ever-growing security challenges across national borders for all countries, in particular developing countries, while noting in this context the strengthening of ITU's role in building confidence and security in the use of ICTs and the need to further enhance international cooperation and capacity-building and develop appropriate existing national, regional and international mechanisms (for example, agreements, best practices, memoranda of understanding, etc.); |

|  |
| --- |
| **IAP/63A1/35 : Inter-American Proposals**  *a)* the crucial importance of information and communication infrastructures, ICTs and their applications for the increase and development of all social and economicactivities; |

|  |
| --- |
| **ARB/72A1/11 : Arab States Common Proposals**  *e)* 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 networks and critical infrastructures continue to give rise to ever-growing security challenges across national borders for all countries, in particular developing countries, while noting in this context the strengthening of ITU's role in building confidence and security in the use of ICTs and the need to further enhance international cooperation and develop appropriate existing national, regional and international mechanisms (for example, international charter, mechanisms, agreements, best practices, memoranda of understanding, etc.); |

|  |
| --- |
| **B/67/4 : Brazil**  *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; |

*d)* that the ITU Secretary-General has been invited to support the International Multilateral Partnership Against Cyber-Threats (IMPACT), the Forum for Incident Response and Security Teams (FIRST) and other global or regional cybersecurity projects, as appropriate, and all countries, particularly developing countries, have been invited to take part in their activities;

|  |
| --- |
| **EUR/48A1/2 : European Common Proposals**  *d)* that the ITU Secretary-General has been invited to support the Forum for Incident Response and Security Teams (FIRST) and other global or regional cybersecurity projects, as appropriate, and all countries, particularly developing countries, have been invited to take part in their activities; |

|  |
| --- |
| **AFCP/55A1/3 : African Common Proposals**  *d)* that the ITU Secretary-General has been invited to global or regional cybersecurity projects such as the Forum for Incident Response and Security Teams (FIRST), as appropriate, and all countries, particularly developing countries, have been invited to take part in their activities; |

|  |
| --- |
| **IAP/63A1/35 : Inter-American Proposals**  *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 networks and ICTs continue to give rise to ever-growing security challenges across national borders for all countries, in particular developing countries, while noting in this context the strengthening of ITU's role in building confidence and security in the use of ICTs and the need to further enhance international cooperation, including through appropriate existing national, regional and international mechanisms (for example, agreements, best practices, memoranda of understanding, etc.);*c)* that the ITU Secretary-General has been invited to support , the Forum for Incident Response and Security Teams (FIRST) and other global or regional cybersecurity projects, as appropriate, and all countries, particularly developing countries, have been invited to take part in their activities; |

|  |
| --- |
| **ARB/72A1/11 : Arab States Common Proposals**  *f)* that the ITU Secretary-General has been invited to support global or regional cybersecurity projects, as appropriate, and all countries, particularly developing countries, have been invited to take part in their activities; |

|  |
| --- |
| **B/67/4 : Brazil**  *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; |

*e)* 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;

|  |
| --- |
| **IAP/63A1/35 : Inter-American Proposals**  *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; |

|  |
| --- |
| **ARB/72A1/11 : Arab States Common Proposals**  *g)* 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; |

|  |
| --- |
| **B/67/4 : Brazil**  *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; |

*f)* 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;

|  |
| --- |
| **EUR/48A1/2 : European Common Proposals**  *f)* that, in order to protect ICTs and address these challenges and threats, cooperative 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, working in cooperation with other stakeholders; |

|  |
| --- |
| **IAP/63A1/35 : Inter-American Proposals**  *e)* that, in order to protect these infrastructures and address these challenges and threats, national, regional and international cooperation is required for protection, detection, 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 working with other organizations and stakeholders;  *f)* that a dynamic, iterative, risk-based approach to cybersecurity enables development and application of cybersecurity practices in a manner that is needed to address constantly evolving threats and vulnerabilities, taking into account the associated risk; |

|  |
| --- |
| **ARB/72A1/11 : Arab States Common Proposals**  *h)* 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, and that ITU has a lead role to play within its mandate and competencies in this field; |

|  |
| --- |
| **B/67/4 : Brazil**  *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; |

*g)* 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;

|  |
| --- |
| **EUR/48A1/2 : European Common Proposals**  *g)* the need for continual evolution in new technologies to support the early detection of, cooperative 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;  *h)* that the technical community and the private sector have lead roles to play in the evolution of technology and that the development and deployment of new technologies and their applications should incorporate holistic approaches in which security is seen as a continuous and iterative process;  *i)* that individuals and organisations have lead roles to play in strengthening cybersecurity, including the adoption of best practices and 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;  *j)* that UNGA Resolution 70/125, the outcome document of the high-level meeting of the General Assembly on the overall review of the implementation of WSIS outcomes, recognized the challenges that States, in particular developing countries, face in building confidence and security in the use of information and communications technologies and called for renewed focus on capacity-building, education, knowledge-sharing and regulatory practice, as well as promoting multi-stakeholder cooperation at all levels and raising awareness among users of information and communications technologies, particularly among the poorest and most vulnerable; |

|  |
| --- |
| **IAP/63A1/35 : Inter-American Proposals**  *g)* the need for continual evolution in new technologies to support the early detection of, and cooperation toward 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; |

|  |
| --- |
| **ARB/72A1/11 : Arab States Common Proposals**  *i)* 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; |

|  |
| --- |
| **B/67/4 : Brazil**  *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; |

*h)* that the number of cyberthreats and cyberattacks is growing, as is dependence on the Internet and other networks that are essential for accessing services and information;

|  |
| --- |
| **EUR/48A1/2 : European Common Proposals**  *k)* that the number of cyberthreats and cyberattacks is growing, as is dependence on the Internet and other networks that are essential for accessing services and information; |

|  |
| --- |
| **ARB/72A1/11 : Arab States Common Proposals**  *j)* that the number of cyberthreats and cyberattacks is growing, as is dependence on the Internet and other networks that are essential for accessing services and information; |

|  |
| --- |
| **B/67/4 : Brazil** |

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

|  |
| --- |
| **EUR/48A1/2 : European Common Proposals**  *l)* that the ITU Telecommunication Standardization Sector (ITU‑T) has adopted around 300 standards relating to building confidence and security in the use of ICTs; |

|  |
| --- |
| **ARB/72A1/11 : Arab States Common Proposals**  *k)* that the ITU Telecommunication Standardization Sector (ITU‑T) is leading the international efforts in building confidence and security in the use of ICTs and has adopted around 300 standards related to cybersecurity; |

|  |
| --- |
| **B/67/4 : Brazil**  *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; |

*j)* 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),

|  |
| --- |
| **EUR/48A1/2 : European Common Proposals**  *m)* that the nature of the cyber-security standards landscape calls for cooperation between organisations such as the ITU, the Internet Engineering Task Force, the International Organisation for Standardisation, the International Electrotechnical Commission and other national, regional, global and sectoral organisations, |

|  |
| --- |
| **IAP/63A1/35 : Inter-American Proposals**  *j)* the final report on Question 3/2 “Securing information and communication networks: Best practices for developing a culture of cybersecurity” of ITU-D;  *k)* that many developing countries are elaborating or implementing national strategies of cybersecurity, |

|  |
| --- |
| **ARB/72A1/11 : Arab States Common Proposals**  *l)* 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);  *m)* the WSIS outcome documents stated that confidence and security are among the main pillars of the Information Society, and it seeks to build confidence and security in the use of ICTs by strengthening the trust framework as part of its commitments to the positive uses of the Internet and other ICTs;  *n)* that security in the cyberspace has become a very important issue in the context of wider international security and that the role and involvement of the United Nations and its relevant specialized agencies such as ITU is therefore becoming increasingly important;  *o)* that the different roles and responsibilities of all stakeholders in ensuring confidence and security in the use if ICTs, and that all stakeholders should act in accordingly;  *p)* that, as stated in the WSIS outcomes, Policy authority for international Internet-related public policy issues is the sovereign right of states and all governments should have an equal role and responsibility for international Internet governance and for ensuring the stability, security and continuity of the existing Internet and its future development and of the future Internet, and that the need for development of public policy by governments in consultation with all stakeholders is also recognized, |

|  |
| --- |
| **B/67/4 : Brazil**  *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

|  |
| --- |
| **ARB/72A1/11 : Arab States Common Proposals**  *a)* that the cyberspace is a fundamental element of securing critical national and international infrastructure and an essential foundation for economic and social online development;  *b)* that international cooperation is essential to tackle the dangers associated with the misuse of information and communications technologies, and that measures are needed to promote, at multilateral levels, the consideration of existing and potential threats, as well as possible strategies to prevent and address them;  *c)* that there is a need to identify collective preventive measures in order to mitigate the effects of illicit use of cyberspace at the global level, particularly in developing countries; |

*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;

|  |
| --- |
| **IAP/63A1/35 : Inter-American Proposals** |

|  |
| --- |
| **ACP/64A1/13 : Asia-Pacific Common Proposals**  *a)* that the development of ICTs has been and continues to be instrumental for the growth and development of the global economy, including the digital economy, underpinned by security and trust; |

|  |
| --- |
| **ARB/72A1/11 : Arab States Common Proposals**  *d)* 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;

|  |
| --- |
| **IAP/63A1/35 : Inter-American Proposals**  *a)* 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; |

|  |
| --- |
| **ARB/72A1/11 : Arab States Common Proposals**  *e)* 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 the Dubai Action Plan and its Objective 3, in particular Output 3.1, on building confidence and security in the use of ICTs, which identifies cybersecurity as a priority activity of the Telecommunication Development Bureau (BDT) and defines the main areas of work to be undertaken by BDT; and has also 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 Resolution 69 (Rev. Dubai, 2014), on the creation of national CIRTs, particularly for developing countries, and cooperation among them;

|  |
| --- |
| **EUR/48A1/2 : European Common Proposals**  *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 Resolution 69 (Rev. Buenos Aires, 2017), on the creation of national CIRTs, particularly for developing countries, and cooperation among them;  *d)* that WTDC‑17 has also adopted the Buenos Aires Action Plan and its Objective 2, which include the aim to strengthen Member States’ capacity to effectively share information, find solutions, and respond to threats to cybersecurity and to develop and implement national strategies and capabilities, including capacity building, encourage national, regional and global cooperation toward enhanced engagement among Member States and relevant players; |

|  |
| --- |
| **AFCP/55A1/3 : African Common Proposals**  *c)* that WTDC‑17 has adopted the Buenos Aires Action Plan and its Objective 2, , on modern and secure telecommunication/ICT infrastructure: foster the development of infrastructure and services, including building confidence and security in the use of telecommunications/ICT and has also 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 Resolution 69 (Rev. Dubai, 2014), on the creation of national CIRTs, particularly for developing countries, and cooperation among them; |

|  |
| --- |
| **IAP/63A1/35 : Inter-American Proposals** |

|  |
| --- |
| **ACP/64A1/13 : Asia-Pacific Common Proposals**  *c)* that WTDC‑17 has adopted the Buenos Aires Action Plan and its Objective 2, on Modern and secure telecommunication/ICT Infrastructure: Foster the development of infrastructure and services, including building confidence and security in the use of telecommunications/ICTs; and has also 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 Resolution 69 (Rev. Buenos Aires, 2017), on the creation of national CIRTs, particularly for developing countries, and cooperation among them; |

|  |
| --- |
| **ARB/72A1/11 : Arab States Common Proposals**  *f)* that WTDC‑17 has adopted the Buenos Aires Action Plan and its Objective 2, on modern and secure telecommunication/ICT infrastructure: foster the development of infrastructure and services, including building confidence and security in the use of telecommunications/ICTs; and has also 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 Resolution 69 (Rev. Buenos Aires, 2017), on the creation of national CIRTs, particularly for developing countries, and cooperation among them;  *g)* that the Buenos Aires Declaration adopted by WTDC-17 declares that: "that building trust, confidence and security in the use of telecommunications/ICTs as well as personal data protection is a priority, with the need for international cooperation and coordination between governments, relevant organizations, private companies and entities in building capacity and exchanging best practices for the development of related public policies and legal, regulatory and technical measures that address, inter alia, personal data protection, and that stakeholders should work together to ensure the reliability and security of ICT networks and services" |

|  |
| --- |
| **B/67/4 : Brazil**  *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. Dubai, 2012), on encouraging the creation of national CIRTs, particularly for developing countries; and WTDC‑14 adopted Resolution 69 (Rev. Dubai, 2014), on the 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;

|  |
| --- |
| **EUR/48A1/2 : European Common Proposals**  *e)* 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. Dubai, 2012), on encouraging the creation of national CIRTs, particularly for developing countries; and WTDC‑14 adopted Resolution 69 (Rev. Dubai, 2014), on the 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; |

|  |
| --- |
| **AFCP/55A1/3 : African Common Proposals** |

|  |
| --- |
| **IAP/63A1/35 : Inter-American Proposals** |

|  |
| --- |
| **ACP/64A1/13 : Asia-Pacific Common Proposals**  *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. Dubai, 2012), on encouraging the creation of national CIRTs, particularly for developing countries; and WTDC‑17 adopted Resolution 69 (Rev. Buenos Aires, 2017), on the 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; |

|  |
| --- |
| **ARB/72A1/11 : Arab States Common Proposals**  *h)* 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 the 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; |

|  |
| --- |
| **B/67/4 : Brazil**  *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*", and that the challenges created by this misuse of ICT resources have only continued to increase since WSIS;

|  |
| --- |
| **EUR/48A1/2 : European Common Proposals** |

|  |
| --- |
| **AFCP/55A1/3 : African Common Proposals**  *d)* that the Buenos Aires Declaration adopted by WTDC-17 declares that: "that building trust, confidence and security in the use of telecommunications/ICTs as well as personal data protection is a priority, with the need for international cooperation and coordination between governments, relevant organizations, private companies and entities in building capacity and exchanging best practices for the development of related public policies and legal, regulatory and technical measures that address, inter alia, personal data protection, and that stakeholders should work together to ensure the reliability and security of ICT networks and services";e) 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. Dubai, 2012), on encouraging the creation of national CIRTs, particularly for developing countries; and WTDC‑14 adopted Resolution 69 (Rev.  Buenos Aires, 2017), on the creation of national CIRTs, including CIRTs responsible for government-to-government cooperation, particularly for developing countries, cooperation among them; *f)* § 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*", and that the challenges created by this misuse of ICT resources have only continued to increase since WSIS; |

|  |
| --- |
| **IAP/63A1/35 : Inter-American Proposals**  *b)* that WTDC‑17 has adopted the Buenos Aires Action Plan and its Objective 2 “Modern and secure telecommunication/ICT Infrastructure: Foster the development of infrastructure and services, including building confidence and security in the use of telecommunications/ICTs”, specifically result 2.2 that establishes the strengthening of the capacity of Member States to effectively share information, find solutions, and respond to threats to cybersecurity, and to develop and implement national strategies and capabilities, including capacity building, encouraging national, regional and international cooperation, *c)* § 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*", and that the challenges created by this misuse of ICT resources have only continued to increase since WSIS; |

|  |
| --- |
| **ARB/72A1/11 : Arab States Common Proposals**  *i)* § 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*", and that the challenges created by this misuse of ICT resources have only continued to increase since WSIS; |

|  |
| --- |
| **B/67/4 : Brazil**  *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;

|  |
| --- |
| **EUR/48A1/2 : European Common Proposals**  *f)* that UNGA Resolution 70/125, the outcome document of the high-level meeting of the General Assembly on the overall review of the implementation of WSIS outcomes, identified several challenges in the implementation of the WSIS action lines that still remain and that will need to be addressed beyond 2015; |

|  |
| --- |
| **AFCP/55A1/3 : African Common Proposals**  *g)* 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; |

|  |
| --- |
| **IAP/63A1/35 : Inter-American Proposals**  *d)* that UNGA resolution 70/125 reaffirmed the importance of building confidence and security in the use of ICTs and the on-going implementation of the outcomes of the World Summit on the Information Society that will require the continued commitment and action of all stakeholders; |

|  |
| --- |
| **ARB/72A1/11 : Arab States Common Proposals**  *j)* 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;

|  |
| --- |
| **EUR/48A1/2 : European Common Proposals**  *h)* that Member States, in particular developing countries, may require assistance from ITU in promoting education and skills development, capacity-building and awareness-raising among businesses and users, aimed at strengthening cybersecurity, on request from these Member States, while noting that there are a number of other regional and international initiatives by all stakeholders which may support these countries; |

|  |
| --- |
| **AFCP/55A1/3 : African Common Proposals**  *h)* 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; |

|  |
| --- |
| **IAP/63A1/35 : Inter-American Proposals**  *e)* 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)* that there are significant capacity building programs underway by and among regional organizations such as the Organization of American States (OAS), the African Union (AUC), the Organization for Security and Cooperation in Europe (OSCE), the ASEAN Regional Forum (ARF), and others as well as by and among Member States, including through the Global Forum for Cyber Expertise (GFCE); |

|  |
| --- |
| **ARB/72A1/11 : Arab States Common Proposals**  *k)* 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, must be offered assistance from ITU, when asked, 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;

|  |
| --- |
| **EUR/48A1/2 : European Common Proposals**  *i)* Opinion 4 (Lisbon, 2009) of the World Telecommunication/ICT Policy Forum, on collaborative strategies for creating confidence and security in the use of ICTs; |

|  |
| --- |
| **AFCP/55A1/3 : African Common Proposals**  *i)* Opinion 4 (Lisbon, 2009) of the World Telecommunication/ICT Policy Forum, on collaborative strategies for creating confidence and security in the use of ICTs; |

|  |
| --- |
| **IAP/63A1/35 : Inter-American Proposals**  *g)* Opinion 4 (Lisbon, 2009) of the World Telecommunication/ICT Policy Forum, on collaborative strategies for creating confidence and security in the use of ICTs; |

|  |
| --- |
| **ARB/72A1/11 : Arab States Common Proposals**  *l)* 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)* the relevant outcomes of WTSA‑12, notably:

|  |
| --- |
| **EUR/48A1/2 : European Common Proposals**  *j)* the relevant outcomes of WTSA‑16, notably: |

|  |
| --- |
| **AFCP/55A1/3 : African Common Proposals**  *j)* the relevant outcomes of WTSA‑12, notably: |

|  |
| --- |
| **IAP/63A1/35 : Inter-American Proposals**  *i)* the relevant outcomes of WTSA‑16, notably: |

|  |
| --- |
| **ACP/64A1/13 : Asia-Pacific Common Proposals**  *i)* the relevant outcomes of WTSA‑16, notably: |

|  |
| --- |
| **ARB/72A1/11 : Arab States Common Proposals**  *i)* the relevant outcomes of WTSA‑16, notably: |

|  |
| --- |
| **B/67/4 : Brazil** |

i) Resolution 50 (Rev. Dubai, 2012), on cybersecurity;

|  |
| --- |
| **EUR/48A1/2 : European Common Proposals**  i) Resolution 50 (Rev. Hammamet, 2016), on cybersecurity; |

|  |
| --- |
| **AFCP/55A1/3 : African Common Proposals**  i) Resolution 50 (Rev. Hammamet, 2016), on cybersecurity; |

|  |
| --- |
| **IAP/63A1/35 : Inter-American Proposals**  i) Resolution 50 (Rev. Hammamet, 2016), on cybersecurity; |

|  |
| --- |
| **ACP/64A1/13 : Asia-Pacific Common Proposals**  i) Resolution 50 (Rev. Hammamet, 2016), on cybersecurity; |

|  |
| --- |
| **ARB/72A1/11 : Arab States Common Proposals**  m) Resolution 50 (Rev. Hammamet, 2016), on cybersecurity; |

|  |
| --- |
| **B/67/4 : Brazil** |

ii) Resolution 52 (Rev. Dubai, 2012), on countering and combating spam,

|  |
| --- |
| **EUR/48A1/2 : European Common Proposals**  ii) Resolution 52 (Rev. Hammamet, 2016), on countering and combating spam, |

|  |
| --- |
| **AFCP/55A1/3 : African Common Proposals**  ii) Resolution 52 (Rev. Hammamet, 2016), on countering and combating spam, |

|  |
| --- |
| **IAP/63A1/35 : Inter-American Proposals**  ii) Resolution 52 (Rev. Hammamet, 2016), on countering and combating spam, |

|  |
| --- |
| **ACP/64A1/13 : Asia-Pacific Common Proposals**  ii) Resolution 52 (Rev. Hammamet, 2016), on countering and combating spam;  *j)* that secure and trusted networks will build confidence and encourage the exchange and use of information and data, |

|  |
| --- |
| **ARB/72A1/11 : Arab States Common Proposals**  ii) Resolution 52 (Rev. Hammamet, 2016), on countering and combating spam, |

|  |
| --- |
| **B/67/4 : Brazil**  *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/67/4 : Brazil**  *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; |

*b)* 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. Dubai, 2012) and Resolutions 45 and 69 (Rev. Dubai, 2014);

|  |
| --- |
| **EUR/48A1/2 : European Common Proposals**  *b)* 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) and Resolutions 45 (Rev. Dubai, 2014) and 69 (Rev. Buenos Aires, 2017); |

|  |
| --- |
| **AFCP/55A1/3 : African Common Proposals**  *b)* 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) and Resolutions 45 and 69 (Rev. Dubai, 2014); |

|  |
| --- |
| **IAP/63A1/35 : Inter-American Proposals**  *b)* 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) and Resolutions 45 (Rev. Dubai, 2014) and 69 (Rev. Buenos Aires, 2017); |

|  |
| --- |
| **ACP/64A1/13 : Asia-Pacific Common Proposals**  *b)* 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) and Resolutions 45(Rev. Dubai, 2014) and 69 (Rev. Buenos Aires, 2017); |

|  |
| --- |
| **ARB/72A1/11 : Arab States Common Proposals**  *b)* 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) and Resolutions 45 and 69 (Rev. Dubai, 2014); |

|  |
| --- |
| **B/67/4 : Brazil**  *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; |

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

|  |
| --- |
| **EUR/48A1/2 : European Common Proposals**  *c)* that, within its mandate, ITU has a fundamental role to play in building confidence and security in the use of ICTs;  *d)* that ITU, as a specialist agency of the United Nations, can play a valuable role in promoting understanding of the landscape of relevant organisations which have important roles to play in strengthening confidence and security in the use of ICTs and promoting cooperation; |

|  |
| --- |
| **IAP/63A1/35 : Inter-American Proposals** |

|  |
| --- |
| **B/67/4 : Brazil**  *d)* that ITU has a fundamental role to play in building confidence and security in the use of ICTs; |

*d)* 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;

|  |
| --- |
| **EUR/48A1/2 : European Common Proposals**  *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; |

|  |
| --- |
| **IAP/63A1/35 : Inter-American Proposals**  *c)* 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; |

|  |
| --- |
| **B/67/4 : Brazil**  *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; |

*e)* 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;

|  |
| --- |
| **EUR/48A1/2 : European Common Proposals**  *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; |

|  |
| --- |
| **IAP/63A1/35 : Inter-American Proposals**  *d)* 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; |

|  |
| --- |
| **B/67/4 : Brazil**  *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; |

*f)* 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;

|  |
| --- |
| **EUR/48A1/2 : European Common Proposals**  *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; |

|  |
| --- |
| **IAP/63A1/35 : Inter-American Proposals**  *e)* 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; |

|  |
| --- |
| **B/67/4 : Brazil**  *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; |

*g)* that WTDC‑14 adopted Resolution 80 (Dubai, 2014), on establishing and promoting trusted information frameworks in developing countries to facilitate and encourage electronic information exchanges between economic partners;

|  |
| --- |
| **EUR/48A1/2 : European Common Proposals**  *h)* that WTDC‑17 adopted Resolution 80 (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; |

|  |
| --- |
| **AFCP/55A1/3 : African Common Proposals**  *g)* that WTDC‑14 adopted Resolution 80 (Rev. Buenos Aires, 2017), on establishing and promoting trusted information frameworks in developing countries to facilitate and encourage electronic information exchanges between economic partners; |

|  |
| --- |
| **IAP/63A1/35 : Inter-American Proposals**  *f)* 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 information exchanges between economic partners; |

|  |
| --- |
| **ACP/64A1/13 : Asia-Pacific Common Proposals**  *g)* that WTDC‑17 adopted Resolution 80 (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; |

|  |
| --- |
| **ARB/72A1/11 : Arab States Common Proposals**  *g)* that WTDC‑17 adopted Resolution 80 (Buenos Aires, 2017), on establishing and promoting trusted information frameworks in developing countries to facilitate and encourage electronic information exchanges between economic partners; |

|  |
| --- |
| **B/67/4 : Brazil**  *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; |

*h)* 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),

|  |
| --- |
| **EUR/48A1/2 : European Common Proposals**  *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), |

|  |
| --- |
| **IAP/63A1/35 : Inter-American Proposals**  *g)* 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), |

|  |
| --- |
| **B/67/4 : Brazil**  *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;

|  |
| --- |
| **ACP/64A1/13 : Asia-Pacific Common Proposals**  *a)* that, as an intergovernmental organization with private‑sector participation, ITU is well-positioned to play an important role, together with other relevant 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;

|  |
| --- |
| **AFCP/55A1/3 : African Common Proposals**  *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, |

|  |
| --- |
| **ARB/72A1/11 : Arab States Common Proposals**  *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, |

|  |
| --- |
| **B/67/4 : Brazil**  *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, |

*d)* the Union's initiative concerning IMPACT and FIRST,

|  |
| --- |
| **EUR/48A1/2 : European Common Proposals**  *d)* the Union's initiative concerning FIRST, |

|  |
| --- |
| **AFCP/55A1/3 : African Common Proposals** |

|  |
| --- |
| **IAP/63A1/35 : Inter-American Proposals**  *d)* the Union's initiative concerning FIRST, |

|  |
| --- |
| **ARB/72A1/11 : Arab States Common Proposals** |

|  |
| --- |
| **B/67/4 : Brazil** |

bearing in mind

|  |
| --- |
| **IAP/63A1/35 : Inter-American Proposals** |

|  |
| --- |
| **B/67/4 : Brazil** |

the work of the ITU established by Resolutions 50, 52 and 58 (Rev. Dubai, 2012); Resolutions 45 and 69 (Rev. Dubai , 2014); Objective 3 of the Dubai Action Plan; the relevant ITU‑T questions on technical aspects regarding the security of information and communication networks; and ITU‑D Question 3/2,

|  |
| --- |
| **EUR/48A1/2 : European Common Proposals**  the work of the ITU established by Resolutions 50, 52 and 58 (Rev. Hammamet, 2016); Resolutions 45 (Rev. Dubai, 2014) and 69 (Rev. Buenos Aires, 2017); Objective 3 of the Dubai Action Plan; the relevant ITU‑T questions on technical aspects regarding the security of information and communication networks; and ITU‑D Question 3/2, |

|  |
| --- |
| **AFCP/55A1/3 : African Common Proposals**  the work of the ITU established by Resolutions 50 and 52 (Rev. Hammamet, 2016) and Resolution 58 (Rev. Dubai, 2012) Resolutions 45 (Rev. Dubai , 2014) and Resolution 69 (Rev. Buenos Aires, 2017); Objective 2 of the Buenos Aires Action Plan; the relevant ITU‑T questions on technical aspects regarding the security of information and communication networks; and ITU‑D Question 3/2, |

|  |
| --- |
| **IAP/63A1/35 : Inter-American Proposals** |

|  |
| --- |
| **ACP/64A1/13 : Asia-Pacific Common Proposals**  the work of the ITU established by Resolutions 50 and 52 (Rev. Hammamet, 2016) and Resolution 58 (Rev. Dubai, 2012); Resolution 45 (Rev. Dubai , 2014) and Resolution 69 (Buenos Aires, 2017); Objective 2 of the Buenos Aires Action Plan; the relevant ITU‑T Questions on technical aspects regarding the security of information and communication networks; and ITU‑D Question 3/2, |

|  |
| --- |
| **ARB/72A1/11 : Arab States Common Proposals**  the work of the ITU established by Resolutions 50, 52 and 58 (Rev. Hammamet, 2016) and Resolution 58 (Rev. Dubai , 2012); Resolutions 45 (Rev. Dubai , 2014) and Resolution 69 (Buenos Aires, 2017); Objective 2 of the Buenos AiresAction Plan; the relevant ITU‑T questions on technical aspects regarding the security of information and communication networks; and ITU‑D Question 3/2,  alarmed by  *a)* the fast growing number of attacks using ICTs, where at the same time increasing dependence on ICTs in providing vital services and managing critical infrastructures;  *b)* the danger of having unsecure and untrusted digital age, which will impact the achievements of the WSIS and 2030 Agenda for SDGs; which are essential to all the world's inhabitants in providing secure, trusted and sustainable social and economic development, |

|  |
| --- |
| **B/67/4 : Brazil** |

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;

|  |
| --- |
| **EUR/48A1/2 : European Common Proposals**  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 and greater awareness of the roles and activities of regional and international organisations involved in strengthening cybersecurity; |

|  |
| --- |
| **ARB/72A1/11 : Arab States Common Proposals**  1 to update the ITU Global Cybersecurity Agenda (GCA) to create a suitable framework, mechanisms and measures, considering existing, potential threats and how to prevent and address them;  2 to start with urgency the development of an international convention on securing cyberspace, taking into account the work of the ITU Sectors;  3 to give this work more high priority within ITU, in accordance with its competences and expertise, including building confidence and security in the use of ICTs at national, regional and more important at the international level; |

2 to give high priority to the work of ITU described under *bearing in mind* above, 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;

|  |
| --- |
| **EUR/48A1/2 : European Common Proposals**  3 to increase understanding of the landscape of regional and global organisations which are involved in strengthening cybersecurity and to support ITU Members to navigate that landscape and to access sources of support and best practice;  4 to raise awareness among other stakeholders, including regional and global organisations, of the particular challenges faced by developing countries, in particular least developed countries and Small Island Developing States, and promote the importance confidence and security in the use of ICTs to sustainable development; |

|  |
| --- |
| **IAP/63A1/35 : Inter-American Proposals**  2 to give high priority to the work of ITU established in Resolutions 50, 52 and 58 (Rev. Dubai, 2012); Resolutions 45 and 69 (Rev. Dubai, 2014); the Objective 2 of the Buenos Aires Action Plan; the relevant ITU-T questions on technical aspects regarding the security of information and communication networks; and ITU‑D Question 3/2,, 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; |

|  |
| --- |
| **ARB/72A1/11 : Arab States Common Proposals**  4 to give high priority to the work of ITU described under *bearing in mind* above, 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; |

|  |
| --- |
| **B/67/4 : Brazil**  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, including Objective 3 and in activities under Question 3/2;

|  |
| --- |
| **EUR/48A1/2 : European Common Proposals**  5 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 information and communication technology;  6 to promote a culture in which security is seen as a continuous and iterative process, built into products from the beginning and continuing throughout their lifetime, and is accessible and understandable for users; |

|  |
| --- |
| **AFCP/55A1/3 : African Common Proposals**  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‑17, including Objective 2 and in activities under Question 3/2; |

|  |
| --- |
| **IAP/63A1/35 : Inter-American Proposals**  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‑17, including Objective 2 and in activities under Question 3/2; |

|  |
| --- |
| **ACP/64A1/13 : Asia-Pacific Common Proposals**  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‑17, including Objective 2 and in activities under Question 3/2; |

|  |
| --- |
| **ARB/72A1/11 : Arab States Common Proposals**  5 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 areas related to Member States application of legal or policy principles at the international level as well as developing technical recommendations designed to prevent vulnerabilities in the ICT infrastructure, and to provide all the assistance that was agreed upon at WTDC‑17, including Objective 2 and in activities under Question 3/2; |

|  |
| --- |
| **B/67/4 : Brazil**  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),

|  |
| --- |
| **EUR/48A1/2 : European Common Proposals**  7 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), |

|  |
| --- |
| **AFCP/55A1/3 : African Common Proposals**  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 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, |

|  |
| --- |
| **IAP/63A1/35 : Inter-American Proposals**  4 to promote greater awareness of and collaboration with entities and initiatives engaged in efforts to improve cybersecurity, including those in *recognizing f*, |

|  |
| --- |
| **ACP/64A1/13 : Asia-Pacific Common Proposals**  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 support the transition of ITU Member States to the digital economy by building confidence and security in the use of ICT, in particular in dealing with existing and future threats, within the mandate of ITU, |

|  |
| --- |
| **ARB/72A1/11 : Arab States Common Proposals**  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 101 (Rev. Busan, 2014), Resolution 102 (Rev. Busan, 2014) and Resolution 140 (Rev. Busan, 2014), |

|  |
| --- |
| **B/67/4 : Brazil**  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, such as the issue of countering spam, which is growing and on the rise;

|  |
| --- |
| **EUR/48A1/2 : European Common Proposals**  i) the work done so far in the three Sectors, under the ITU Global Cybersecurity Agenda and in other relevant organizations and initiatives to strengthen protection against existing and future threats in order to build confidence and security in the use of ICTs, such as the issue of countering spam, which is growing and on the rise; |

|  |
| --- |
| **ARB/72A1/11 : Arab States Common Proposals**  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, such as the issue of preventing threats, which is growing and on the rise; |

|  |
| --- |
| **B/67/4 : Brazil**  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;

|  |
| --- |
| **EUR/48A1/2 : European Common Proposals**  iii) the results of work done so far to support developing countries in particular to build capacity and skills in cybersecurity in order to ensure that the ITU is effectively focusing its resources to address development challenges; |

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;

|  |
| --- |
| **EUR/48A1/2 : European Common Proposals**  4 to raise awareness among other stakeholders, including regional and global organisations and stakeholders from the private sector and technical community, of the particular challenges faced by developing countries in building confidence and security in the use of ICTs so that it can inform their work and activities with developing countries; |

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;

|  |
| --- |
| **EUR/48A1/2 : European Common Proposals**  5 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;

|  |
| --- |
| **EUR/48A1/2 : European Common Proposals**  6 to share information among Member States on the tools and resources available from other regional and global organisations to build confidence and security in the use of ICTs and support Member States to access them, including maintaining 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;

|  |
| --- |
| **EUR/48A1/2 : European Common Proposals**  7 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,

|  |
| --- |
| **EUR/48A1/2 : European Common Proposals**  8 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‑12, particularly Resolutions 50, 52 and 58 (Rev. Dubai, 2012), allowing work to begin before a question is approved;

|  |
| --- |
| **EUR/48A1/2 : European Common Proposals**  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, 52 and 58 (Rev. Hammamet, 2016); |

|  |
| --- |
| **AFCP/55A1/3 : African Common Proposals**  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‑12, particularly Resolutions 50 and 52 (Rev. Hammamet, 2016) and 58 (Rev. Dubai, 2012), allowing work to begin before a question is approved; |

|  |
| --- |
| **IAP/63A1/35 : Inter-American Proposals**  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, 52 (Rev. Hammamet, 2016) and 58 (Rev. Dubai, 2012), allowing work to begin before a question is approved; |

|  |
| --- |
| **ACP/64A1/13 : Asia-Pacific Common Proposals**  i) address existing and future threats and vulnerabilities affecting efforts to build confidence and security in the use of ICTs, taking into account new services and emerging applications based on telecommunication/ICT networks, 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 Resolution 58 (Rev. Dubai, 2012), allowing work to begin before a question is approved; |

|  |
| --- |
| **ARB/72A1/11 : Arab States Common Proposals**  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, 52 (Rev. Hammamet, 2016) and 58 (Rev. Dubai, 2012), allowing work to begin before a question is approved; |

|  |
| --- |
| **B/67/4 : Brazil**  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:

|  |
| --- |
| **EUR/48A1/2 : European Common Proposals**  iii) facilitate projects deriving from the outcomes of WTSA‑16, in particular: |

|  |
| --- |
| **IAP/63A1/35 : Inter-American Proposals**  iii) facilitate projects deriving from the outcomes of WTSA‑16, in particular: |

|  |
| --- |
| **ACP/64A1/13 : Asia-Pacific Common Proposals**  iii) facilitate projects deriving from the outcomes of WTSA‑16, in particular: |

|  |
| --- |
| **ARB/72A1/11 : Arab States Common Proposals**  iii) facilitate projects deriving from the outcomes of WTSA‑16, in particular: |

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

• Resolution 52 (Rev. Dubai, 2012), on countering and combating spam;

|  |
| --- |
| **EUR/48A1/2 : European Common Proposals**  • Resolution 52 (Rev. Hammamet, 2016), on countering and combating spam;  2 to consider how ITU-T can promote a culture in which security is seen as a continuous and iterative process, and to make proposals to Council as appropriate; |

|  |
| --- |
| **AFCP/55A1/3 : African Common Proposals**  • Resolution 52 (Rev.  Hammamet, 2016), on countering and combating spam; |

|  |
| --- |
| **IAP/63A1/35 : Inter-American Proposals**  • Resolution 52 (Rev. Hammamet, 2016), on countering and combating spam; |

|  |
| --- |
| **ACP/64A1/13 : Asia-Pacific Common Proposals**  • Resolution 52 (Rev. Hammamet, 2016), on countering and combating spam; |

|  |
| --- |
| **ARB/72A1/11 : Arab States Common Proposals**  • Resolution 52 (Rev. Hammamet, 2016), on countering and combating spam; |

|  |
| --- |
| **B/67/4 : Brazil**  • 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,

|  |
| --- |
| **EUR/48A1/2 : European Common Proposals**  3 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, |

|  |
| --- |
| **IAP/63A1/35 : Inter-American Proposals**  2 to continue collaboration with relevant organizations with a view to exchanging best practices and disseminating information through such mechanisms as, 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 and 69 (Rev. Dubai, 2014), Resolution 80 (Dubai, 2014) and Objective 3 of the Dubai Action Plan, to support ongoing regional and global cybersecurity projects, and to encourage all countries to take part in these activities;

|  |
| --- |
| **EUR/48A1/2 : European Common Proposals**  1 consistent with the results of WTDC‑17 and pursuant to Resolutions 45 (Rev. Dubai, 2014), Resolution 69 and Resolution 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; |

|  |
| --- |
| **AFCP/55A1/3 : African Common Proposals**  1 consistent with the results of WTDC‑17 and pursuant to Resolutions 45 (Rev. Dubai, 2014) and Resolution 69 (Rev. Buenos Aires, 2017), Resolution 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; |

|  |
| --- |
| **IAP/63A1/35 : Inter-American Proposals**  1 consistent with the results of WTDC‑17 and pursuant to Resolutions 45 (Rev. Dubai, 2014) and 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; |

|  |
| --- |
| **ACP/64A1/13 : Asia-Pacific Common Proposals**  1 consistent with the results of WTDC‑17 and pursuant to Resolutions 45 (Rev. Dubai, 2014) and Resolution 69 (Rev. Buenos Aires, 2017), Resolution 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; |

|  |
| --- |
| **ARB/72A1/11 : Arab States Common Proposals**  1 consistent with the results of WTDC‑17 and pursuant to Resolutions 45 (Rev. Dubai, 2014) and Resolution 69 (Rev. Buenos Aires, 2017), Resolution 80 (Rev. Buenos, 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; |

|  |
| --- |
| **B/67/4 : Brazil**  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;

|  |
| --- |
| **EUR/48A1/2 : European Common Proposals**  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 to build confidence and security in the use of ICTs; supporting ITU Member States' national and regional efforts to build capacity to protect against cyberthreats/cybercrime, in collaboration with one another; supporting ITU Member States’ efforts to raise awareness among organisations and individual users of the important role they play in strengthening cybersecurity; 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; supporting Member States’ efforts to establish 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; supporting the establishment of 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;

|  |
| --- |
| **IAP/63A1/35 : Inter-American Proposals**  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 approved by ITU Council; |

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;

|  |
| --- |
| **AFCP/55A1/3 : African Common Proposals**  7 to support the work of SG17 and other ITU-T Study Groups by promoting and encouraging ITU Member States and Sector Members especially from developing countries to deploy approved security related ITU-T Recommendations; |

|  |
| --- |
| **ARB/72A1/11 : Arab States Common Proposals**  7 to support the work of SG17 and other ITU-T Study Groups by continuing promote and encourage ITU Member States and Sector Members especially from developing countries to deploy approved security related ITU-T Recommendations; |

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 Dubai Action Plan;

|  |
| --- |
| **EUR/48A1/2 : European Common Proposals**  7 to support ITU Member States in the development of their national and/or regional cybersecurity strategies toward building national capabilities for protection against and dealing with cyberthreats in accordance with the principles of international cooperation, consistent with Objective 2 of the Buenos Aires Action Plan; |

|  |
| --- |
| **AFCP/55A1/3 : African Common Proposals**  8 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  2 of the Buenos Aires Action Plan; |

|  |
| --- |
| **IAP/63A1/35 : Inter-American Proposals**  7 to support ITU Member States in the development of their national and/or regional cybersecurity strategies, toward building national capabilities to improve cybersecurity and address evolving threats in accordance with the principles of international cooperation, consistent with Objective 2 of the Buenos Aires Action Plan; |

|  |
| --- |
| **ACP/64A1/13 : Asia-Pacific Common Proposals**  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 2 of the Buenos Aires Action Plan; |

|  |
| --- |
| **ARB/72A1/11 : Arab States Common Proposals**  8 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 2 of the Buenos Aires Action Plan; |

|  |
| --- |
| **B/67/4 : Brazil**  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; |

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

|  |
| --- |
| **AFCP/55A1/3 : African Common Proposals**  9 to report annually to the Council on these activities and make proposals as appropriate, |

|  |
| --- |
| **B/67/4 : Brazil**  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‑12 and WTDC‑14, including the programme described in Output 3.1 of Objective 3 of the Dubai Action Plan, on providing support and assistance to developing countries in building confidence and security in the use of ICTs;

|  |
| --- |
| **EUR/48A1/2 : European Common Proposals**  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; |

|  |
| --- |
| **AFCP/55A1/3 : African Common Proposals**  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; |

|  |
| --- |
| **IAP/63A1/35 : Inter-American Proposals**  1 to implement relevant resolutions of both WTSA‑16 and WTDC‑17, included output 2.2 of the Objective 2 of the Buenos Aires Action Plan, with a particular focus on the needs of developing countries as they undertake efforts to improve cybersecurity and build confidence and security in the use of ICTs; |

|  |
| --- |
| **ACP/64A1/13 : Asia-Pacific Common Proposals**  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; |

|  |
| --- |
| **ARB/72A1/11 : Arab States Common Proposals**  1 to implement relevant resolutions of both WTSA‑16 and WTDC‑17, including the programme described 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; |

|  |
| --- |
| **B/67/4 : Brazil**  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;

|  |
| --- |
| **EUR/48A1/2 : European Common Proposals**  2 to identify and promote the availability of information on building confidence and security in the use of ICTs, 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;

|  |
| --- |
| **IAP/63A1/35 : Inter-American Proposals**  3 to contribute to the work of 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;

|  |
| --- |
| **ARB/72A1/11 : Arab States Common Proposals**  4 to cooperate with relevant organizations and other relevant international and national experts, as appropriate, in order to identify best practices in building confidence and security in the use of ICTs, including 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;

|  |
| --- |
| **EUR/48A1/2 : European Common Proposals**  6 to identify and document practical steps to support developing countries to build capacity and skills in cybersecurity, taking into account the specific challenges they face;  7 to take into account the challenges faced by stakeholders from the private sector, civil society and the technical community, particularly in developing countries, to build confidence and security in the use of ICTs and identify steps that can help to address them; |

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;

|  |
| --- |
| **EUR/48A1/2 : European Common Proposals**  8 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 and other stakeholders 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;  9 to identify and document practical steps to strengthen security in the use of ICTs internationally, based on widely accepted practices, guidelines and recommendations, that other stakeholders can choose to apply to improve their ability to protect against and deal with cyberthreats and attacks; |

|  |
| --- |
| **IAP/63A1/35 : Inter-American Proposals**  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 including a dynamic and iterative risk-based approach that reflects the evolving nature of threats and vulnerabilities, 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;

|  |
| --- |
| **EUR/48A1/2 : European Common Proposals**  10 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);

|  |
| --- |
| **EUR/48A1/2 : European Common Proposals**  11 to provide the necessary technical and financial support, within the constraints of existing budgetary resources, in accordance with Resolution 58 (Rev. Dubai, 2012); |

|  |
| --- |
| **B/67/4 : Brazil**  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; |

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

|  |
| --- |
| **EUR/48A1/2 : European Common Proposals**  12 to mobilize appropriate extrabudgetary resources, outside the regular budget of the Union, for the implementation of this resolution, to help developing countries, |

|  |
| --- |
| **ARB/72A1/11 : Arab States Common Proposals**  9 to mobilize appropriate extrabudgetary resources, outside the regular budget of the Union, for the implementation of this resolution, to help developing countries;  10 to support and assist Developing countries in deploying Security related ITU-T Recommendations;  11 to take into account in their relevant work the challenges and issues faced by member states especially those from developing countries in building confidence and security in the use of ICTs and identify actions that can help to address them, |

|  |
| --- |
| **B/67/4 : Brazil**  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:

|  |
| --- |
| **ARB/72A1/11 : Arab States Common Proposals**  1 to bring to the attention of UNGA in its 73rd session the adoption of this resolution and to highlight the leading role of the union at the international level in the field of ICTs in the context of confidence and security;  2 to take concrete actions to ensure wider adoption for the international convention related to securing cyberspace; |

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;

|  |
| --- |
| **IAP/63A1/35 : Inter-American Proposals**  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 assisting Member States with building confidence and security in the use of ICTs; |

|  |
| --- |
| **ARB/72A1/11 : Arab States Common Proposals**  3 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,

|  |
| --- |
| **EUR/48A1/2 : European Common Proposals**  2 to cooperate with relevant international organizations, |

|  |
| --- |
| **ARB/72A1/11 : Arab States Common Proposals**  4 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

|  |
| --- |
| **ARB/72A1/11 : Arab States Common Proposals**  instructs the Council Working Group on international Internet-related public policy issues  1 to study the international issues raised in this resolution and to develop international Internet-related public policy, as a matter of urgency, in order to address them appropriately;  2 to submit annually to council the progress made in developing and implementing the above mentioned international public policy, invites Member States  1 to participate actively in establishing the appropriate international convention allowing rapid response to major incidents, and propose an action plan to prevent and mitigate such incidents; |

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

|  |
| --- |
| **ARB/72A1/11 : Arab States Common Proposals**  2 to consider developing appropriate competent international and regional initiatives for establishing international 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;

|  |
| --- |
| **ARB/72A1/11 : Arab States Common Proposals**  3 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;

|  |
| --- |
| **EUR/48A1/2 : European Common Proposals**  4 to raise awareness among all stakeholders, including organisations and individual users, of the importance of basic safeguards as a critical element in strengthening cybersecurity;  5 to promote a culture in which security is seen as a continuous and iterative process, particularly in cooperation with the private sector and technical community;  6 to access the resources, support and best practice available from regional and global organisations involved in cybersecurity to support countries to build confidence and security in the use of ICTs; |

|  |
| --- |
| **ARB/72A1/11 : Arab States Common Proposals**  4 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,

|  |
| --- |
| **EUR/48A1/2 : European Common Proposals**  7 to inform the Secretary-General of relevant activities related to this resolution regarding confidence and security in the use of ICTs, |

|  |
| --- |
| **IAP/63A1/35 : Inter-American Proposals**  4 to inform the Secretary-General of relevant activities related to this resolution regarding confidence and security in the use of ICTs;  5 to collaborate closely with relevant organizations, through the exchange of best practices for the development and implementation of national CIRTS, |

|  |
| --- |
| **ARB/72A1/11 : Arab States Common Proposals**  5 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

|  |
| --- |
| **ARB/72A1/11 : Arab States Common Proposals**  6 to participate actively in the work of CWG-Internet related to this resolution,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;

|  |
| --- |
| **ARB/72A1/11 : Arab States Common Proposals**  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 the WSIS Outcome Documents, WSIS+10 Statement on the Implementation of WSIS Outcomes and the WSIS+10 Vision for WSIS Beyond 2015, the outcome document of the high-level meeting of the General Assembly on the overall review of the implementation of WSIS outcomes and to contribute to the preparation and implementation of those activities; |

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

|  |
| --- |
| **EUR/48A1/2 : European Common Proposals**  3 to promote the development of educational and training programmes to enhance user awareness of risks in cyberspace and the steps that users can take to protect themselves; |

|  |
| --- |
| **IAP/63A1/35 : Inter-American Proposals**  4 to incorporate a dynamic and iterative risk-based approach toward addressing evolving threats and vulnerabilities in their efforts to build confidence and security in the use of ICTs; |

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

|  |
| --- |
| **IAP/63A1/35 : Inter-American Proposals**  5 to collaborate, as appropriate, in order to address and prevent problems that undermine confidence and security in the use of telecommunications/ICTs. |

|  |
| --- |
| **ARB/72A1/11 : Arab States Common Proposals**  4 to collaborate, as appropriate, in order to address and prevent international and national problems that undermine confidence and security in the use of telecommunications/ICTs;  5 to provide financial and human resources and expertise to support the Union in implementing of the actions a raised from this resolution. |

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-3)
3. 1 These include the least developed countries, small island developing states, landlocked developing countries and countries with economies in transition. [↑](#footnote-ref-4)
4. 1 These include the least developed countries, small island developing states, landlocked developing countries and countries with economies in transition. [↑](#footnote-ref-5)
5. 1 These include the least developed countries, small island developing states, landlocked developing countries and countries with economies in transition. [↑](#footnote-ref-6)
6. 1 These include the least developed countries, small island developing states, landlocked developing countries and countries with economies in transition. [↑](#footnote-ref-7)