Inter-Parliamentary Union
For democracy. For everyone.

146TH IPU ASSEMBLY
المنامة، البحرين
MANAMA, BAHRAIN
11-15 MARCH 2023 - ١١-١٥ مارس ٢٠٢٣

146th IPU Assembly
Manama (11–15 March 2023)

Standing Committee on
Peace and International Security

C-I/146/DR-am
6 March 2023

Cyberattacks and cybercrimes: The new risks to global security

<u>Amendments to the draft resolution</u> submitted within the statutory deadline by Argentina, Belgium, Canada, Czech Republic, Egypt, Finland, France, Germany, India, Iran (Islamic Republic of), Japan, Lithuania, Nicaragua, Pakistan, Philippines, Republic of Korea, Romania, Russian Federation, Singapore, South Africa, South Sudan, Sweden, Switzerland, Thailand, Türkiye, Ukraine and Viet Nam

PREAMBULAR

<u>Preambular paragraph 1</u>

Amend to read as follows:

(1) *Condemning* all forms of ~~cybercrime~~ **the use of information and communications technologies for criminal purposes** and cyberattacks**,** and *reaffirming* the need to combat such acts through international cooperation and the development of effective**,** ~~legal~~ **international, legally binding** frameworks **tailored to the unique attributes of information and communications technologies (ICTs)**, **1**

(Islamic Republic of Iran)

Amend to read as follows:

(1) *Condemning* all forms of ~~cybercrime~~ **misuse of ICT for criminal purposes** and cyberattacks and *reaffirming* the need to combat such acts through international cooperation and the development of effective legal frameworks, **2**

(Pakistan)

E

#IPU146

Amend to read as follows:

(1) *Condemning* all forms of **the use of information and communications technologies for criminal purposes, hereinafter referred to as "**cybercrime**",** and **computer attacks, hereinafter referred to as "**cyberattacks**",** and *reaffirming* the need to combat such acts through international cooperation and the development of effective legal frameworks, **3**

(Russian Federation)

Amend to read as follows:

(1) *Condemning* all forms of cybercrime ~~and cyberattacks~~ and *reaffirming* the need to combat such acts through international cooperation and the development of effective legal frameworks, **4**

(Czech Republic, Sweden)

Amend to read as follows:

(1) *Condemning* all forms of cybercrime and ~~cyberattacks~~ **cyber incidents** and *reaffirming* the need to combat such acts through international cooperation and the development of effective legal frameworks, **5**

(India)

Amend to read as follows:

(1) *Condemning* all forms of cybercrime and **malicious** cyberattacks and *reaffirming* the need to combat such ~~acts~~ **crimes** through international cooperation and the development of effective legal frameworks, **6**

(Belgium)

Amend to read as follows:

(1) *Condemning* all forms of cybercrime and cyberattacks ~~and *reaffirming* the need to combat such acts through international cooperation and the development of effective legal frameworks~~ **together with all heinous crimes associated with them**, **7**

(South Sudan)

Amend to read as follows:

(1) *Condemning* all forms of cybercrime and cyberattacks and *reaffirming* the need to combat such acts through international cooperation ~~and the development of effective legal frameworks~~, **8**

(Germany)

Amend to read as follows:

(1) *Condemning* all forms of cybercrime and cyberattacks and *reaffirming* the need to combat such acts through international cooperation and ~~the development of~~ effective legal ~~frameworks~~ **discussions**, **9**

(Japan)

Amend to read as follows:

(1) *Condemning* all forms of cybercrime and cyberattacks and *reaffirming* the need to combat such acts through international cooperation **and coordination among stakeholders both within and between countries**, **including the sharing of information on cybercrime threats,** and the development of effective legal frameworks, **10**

(South Africa)

Amend to read as follows:

(1) *Condemning* all forms of cybercrime and cyberattacks and *reaffirming* the need to combat such acts through international cooperation and the **application or, where necessary,** development of effective legal frameworks, **11**

(Switzerland)

Amend to read as follows:

(1) *Condemning* all forms of cybercrime and cyberattacks and *reaffirming* the need to combat such acts through international cooperation and the development of effective legal frameworks **that reflect the rules-based international system**, **12**

(Canada)

New preambular paragraph 1bis

(1bis) *Acknowledging* that cybercrime and cyberattacks are distinct yet interrelated phenomena of a criminal nature in the digital era, associated with different scopes of malicious uses of information and communications technologies, **13**

(Argentina)

(1bis) *Reaffirming* the existing United Nations framework for responsible State behaviour in the use of ICTs and the need to implement this framework, **14**

(Germany)

(1bis) *Affirming* the need to combat such acts through national, regional and international cooperation and the development of effective legal frameworks, **15**

(South Sudan)

Preambular paragraph 2

Amend to read as follows:

(2) *Recognizing* the need to build trust between countries ~~in response to cybercriminals, who recognize neither boundaries nor borders~~ **to address risks to cybersecurity**, **16**

(India)

Amend to read as follows:

(2) *Recognizing* the need to build trust between countries in response to ~~cybercriminals~~ **the malicious use of ICTs by State as well as non-State actors**, who recognize neither boundaries nor borders, **17**

(Germany)

Amend to read as follows:

(2) *Recognizing* the need to build trust between countries in response to cybercriminals **and malicious actors**, who recognize neither boundaries nor borders, **18**

(Islamic Republic of Iran)

Amend to read as follows:

(2) *Recognizing* the need to build trust **and mutual understanding** between countries in response to cybercriminals, who recognize neither boundaries nor borders, **19**

(Thailand)

Preambular paragraph 3

Amend to read as follows:

(3) *Observing* the growing **use of and** dependence on ~~cyberspace among individuals, institutions and States~~ **ICTs worldwide**, **20**

(Germany)

Amend to read as follows:

(3) *Observing* the growing dependence on ~~cyberspace~~ **the ICT environment** among individuals, institutions and States, **21**

(Islamic Republic of Iran)

Amend to read as follows:

(3) *Observing* the growing dependence on **the space in which information and communications technologies are used, hereinafter referred to as "**cyberspace**",** among individuals, institutions and States, **22**

(Russian Federation)

Preambular paragraph 4

Amend to read as follows:

(4) *Cognizant of* the increase in ~~cybercrime~~ **the use of information and communications technologies for criminal purposes** and ~~cyberattacks~~ **ICT threat** due to increasing digitalization, especially the forced digitalization imposed by the COVID-19 pandemic, **23**

(Islamic Republic of Iran)

Amend to read as follows:

(4) *Cognizant of* the increase in ~~cybercrime~~ **misuse of ICT for criminal purposes** and cyberattacks due to increasing digitalization, especially the forced digitalization imposed by the COVID-19 pandemic, **24**

(Pakistan)

Amend to read as follows:

(4) *Cognizant of* the increase in cybercrime ~~and cyberattacks~~ due to increasing digitalization~~, especially the forced digitalization imposed by~~ **during and following** the COVID-19 pandemic, **25**

(Czech Republic)

Amend to read as follows:

(4) *Cognizant of* the increase in cybercrime and ~~cyberattacks~~ **its increasing application in cyberwarfare operations, such as decoy ransomware leveraged for destructive cyberattacks on critical civilian infrastructure,** due to increasing digitalization, especially the forced digitalization imposed by the COVID-19 pandemic, **26**

(Sweden)

Amend to read as follows:

(4) *Cognizant of* the increase in cybercrime and ~~cyberattacks~~ **cyber incidents** due to increasing digitalization, especially ~~the forced digitalization imposed by~~ **since the onset of** the COVID-19 pandemic, **27**

(India)

Amend to read as follows:

(4) *Cognizant of* the increase in cybercrime **activities** and cyberattacks due to increasing digitalization, ~~especially the forced digitalization imposed~~ **accelerated** by the COVID-19 pandemic, **28**

(Germany)

Amend to read as follows:

(4) *Cognizant of* the increase in cybercrime and **malicious** cyberattacks due to increasing digitalization, especially the ~~forced~~ digitalization imposed by the COVID-19 pandemic, **29**

(Belgium)

Amend to read as follows:

(4) *Cognizant of* the increase in cybercrime and cyberattacks due to increasing digitalization, especially the ~~forced~~ digitalization imposed by the COVID-19 pandemic, **30**

(Lithuania)

Amend to read as follows:

(4) *Cognizant of* the increase in cybercrime and cyberattacks **on the critical infrastructure of States and of enterprises supporting essential services to the public, as well as on the well-being of individuals,** due to increasing digitalization, especially the forced digitalization imposed by the COVID-19 pandemic, **31**

(South Africa)

New preambular paragraph 4bis

(4bis) *Also cognizant* of the challenges faced by States in combating cyberattacks and cybercrime, and *emphasizing* the need to reinforce technical assistance and capacity-building activities, upon request, to strengthen the ability of national authorities to deal with cyberattacks and cybercrime, **32**

(South Africa)

Preambular paragraph 5

Amend to read as follows:

(5) *Noting* the responsibility of parliaments to protect citizens in ~~cyberspace~~ **the ICT environment** with new infrastructure and resources, in the same way as in the physical world, **33**

(Islamic Republic of Iran)

Amend to read as follows:

(5) *Noting* the responsibility of parliaments to protect citizens in cyberspace ~~with new infrastructure and resources,~~ in the same way as in the physical world, **34**

(India)

Amend to read as follows:

(5) *Noting* the responsibility of parliaments to ~~protect~~ **build a regulatory framework that protects** citizens in cyberspace with new infrastructure and resources, in the same way as in the physical world, **35**

(Argentina)

Amend to read as follows:

(5) *Noting* the responsibility of parliaments to ~~protect~~ **ensure the protection of their** citizens in cyberspace with new infrastructure and resources, in the same way as in the physical world, **36**

(Thailand)

Amend to read as follows:

(5) *Noting* the ~~responsibility~~ **role** of parliaments to protect citizens in cyberspace with new infrastructure and resources, in the same way as in the physical world, **37**

(Lithuania)

Amend to read as follows:

(5) *Noting* the responsibility of parliaments to protect citizens in cyberspace with new infrastructure and resources, in the same way as in the physical world, **where they do not yet exist in their country**, **38**

(Nicaragua)

New preambular paragraph 5bis

(5bis) *Recognizing* that, in light of the pace of global technological developments, new policy and legal frameworks must likewise be swiftly and comprehensively developed, **39**

(Philippines)

(5bis) *Reaffirming* that the United Nations has a leading role in facilitating dialogue on the use of information and communications technologies by States, pursuant to United Nations General Assembly resolution 76/19, **40**

(Russian Federation)

(5bis) *Emphasizing* the dependence on digital technology platforms and infrastructure, along with the risk of cyberattacks, when governments deploy online public service applications, **41**

(Viet Nam)

New preambular paragraph 5ter

(5ter) *Supporting* the Open-ended Working Group on security of and in the use of information and communications technologies 2021–2025, and *recognizing* its mandate pursuant to United Nations General Assembly resolution 75/240, **42**

(Russian Federation)

(5ter) *Affirming* the view that the protection of human rights in the cyber world is similar to in the real one, in line with the international commitments of United Nations Member States, **43**

(Viet Nam)

Preambular paragraph 6

Amend to read as follows:

(6) *Recalling* United Nations General Assembly resolution 31/72 of 10 December 1976 on the *Convention on the Prohibition of Military or Any Other Hostile Use of Environmental Modification Techniques*, resolutions 55/63 of 4 December 2000 and 56/121 of 19 December 2001 on *Combating the criminal misuse of information technologies*, ~~resolution 57/239 of 31 January 2003 on the *Creation of a global culture of cybersecurity*, and resolution~~ **resolutions** 69/28 of 2 December 2014**, 70/237 of 23 December 2015, 71/28 of 5 December 2016, 73/27 of 5 December 2018, 74/29 of 12 December 2019, 75/240 of 31 December 2020 and 77/36 of 7 December 2022** on *Developments in the field of information and telecommunications in the context of international security*, **and resolution 76/19 of 6 December 2021 *on Developments in the field of information and telecommunications in the context of international security, and advancing responsible State behaviour in the use of information and communications technologies,** **44**

(Russian Federation)

Amend to read as follows:

(6) *Recalling* United Nations General Assembly resolution 31/72 of 10 December 1976 on the *Convention on the Prohibition of Military or Any Other Hostile Use of Environmental Modification Techniques*, resolutions 55/63 of 4 December 2000 and 56/121 of 19 December 2001 on *Combating the criminal misuse of information technologies*, resolution 57/239 of 31 January 2003 on the *Creation of a global culture of cybersecurity*, ~~and~~ resolution ~~69/28 of 2 December 2014 on *Developments in the field of information and telecommunications in the context of international security*~~ **76/19 of 6 December 2021 on *Developments in the field of information and telecommunications in the context of international security, and advancing responsible State behaviour in the use of information and communications technologies*, resolution 77/36 of 7 December 2022 on *Developments in the field of information and telecommunications in the context of international security*, and resolution 77/37 of 7 December 2022 on a *Programme of action to advance responsible State behaviour in the use of information and communications technologies in the context of international security***, **45**

(Egypt)

Amend to read as follows:

(6) *Recalling* United Nations General Assembly resolution 31/72 of 10 December 1976 on the *Convention on the Prohibition of Military or Any Other Hostile Use of Environmental Modification Techniques*, resolutions 55/63 of 4 December 2000 and 56/121 of 19 December 2001 on *Combating the criminal misuse of information technologies*, resolution 57/239 of 31 January 2003 on the *Creation of a global culture of cybersecurity*, and ~~resolution~~ **resolutions** 69/28 of 2 December 2014, **73/27 of 5 December 2018, 75/240 of 31 December 2020 and 77/36 of 7 December 2022** on *Developments in the field of information and telecommunications in the context of international security*, **46**

(Islamic Republic of Iran)

Amend to read as follows:

(6) *Recalling* United Nations General Assembly resolution 31/72 of 10 December 1976 on the *Convention on the Prohibition of Military or Any Other Hostile Use of Environmental Modification Techniques*, resolutions 55/63 of 4 December 2000 and 56/121 of 19 December 2001 on *Combating the criminal misuse of information technologies*, resolution 57/239 of 31 January 2003 on the *Creation of a global culture of cybersecurity*, and resolution 69/28 of 2 December 2014 on *Developments in the field of information and telecommunications in the context of international security**,*** **as well as the consensus final reports of 2021 of the United Nations Open-ended Working Group on developments in the field of information and telecommunications in the context of international security, and of the United Nations Group of Governmental Experts on advancing responsible State behaviour in the context of international security**, **47**

(Germany)

Amend to read as follows:

(6) *Recalling* United Nations General Assembly resolution 31/72 of 10 December 1976 on the *Convention on the Prohibition of Military or Any Other Hostile Use of Environmental Modification Techniques*, resolutions 55/63 of 4 December 2000 and 56/121 of 19 December 2001 on *Combating the criminal misuse of information technologies*, resolution 57/239 of 31 January 2003 on the *Creation of a global culture of cybersecurity*, ~~and~~ resolution 69/28 of 2 December 2014 on *Developments in the field of information and telecommunications in the context of international security*, **and resolution 73/266 of 22 December 2018 on *Advancing responsible State behaviour in cyberspace in the context of international security***, **48**

(Thailand)

New preambular paragraph 6bis

(6bis) *Also recalling* United Nations General Assembly resolution 70/237 of 23 December 2015, also on *Developments in the field of information and telecommunications in the context of international security*, which endorsed the voluntary and non-binding norms regarding responsible State behaviour in the use of information and communications technologies developed by the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, and called on Member States to be guided by these norms, **49**

(Canada)

Preambular paragraph 7

Amend to read as follows:

(7) *Stressing* the importance of regional conventions on ~~cybercrime, transnational organized crime~~ **the use of information and communications technologies for criminal purposes, and on the** exchange of information and administrative assistance, including the Council of Europe *Convention on Cybercrime* of 23 November 2001 and its *Additional Protocol concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems* of 28 January 2003, the *Agreement on Cooperation in Ensuring International Information Security between the Member States of the Shanghai Cooperation Organization* of 16 June 2009, and the *Arab Convention on Combating Information Technology Offences* of 21 December 2010, **50**

(Islamic Republic of Iran)

Amend to read as follows:

(7) *Stressing* the importance of regional conventions on ~~cybercrime~~ **misuse of ICT for criminal purposes**, transnational organized crime, exchange of information and administrative assistance, including the Council of Europe *Convention on Cybercrime* of 23 November 2001 and its *Additional Protocol concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems* of 28 January 2003, the *Agreement on Cooperation in Ensuring International Information Security between the Member States of the Shanghai Cooperation Organization* of 16 June 2009, and the *Arab Convention on Combating Information Technology Offences* of 21 December 2010, **51**

(Pakistan)

Amend to read as follows:

(7) *Stressing* the importance of regional conventions on cybercrime, transnational organized crime, exchange of information and administrative assistance, ~~including the Council of Europe *Convention on Cybercrime* of 23 November 2001 and its *Additional Protocol concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems* of 28 January 2003, the *Agreement on Cooperation in Ensuring International Information Security between the Member States of the Shanghai Cooperation Organization* of 16 June 2009, and the *Arab Convention on Combating Information Technology Offences* of 21 December 2010,~~ **52**

(India)

Amend to read as follows:

(7) ~~*Stressing* the importance~~ ***Taking note*** of regional conventions on cybercrime, transnational organized crime, exchange of information and administrative assistance, including the Council of Europe *Convention on Cybercrime* of 23 November 2001 and its *Additional Protocol concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems* of 28 January 2003, the *Agreement on Cooperation in Ensuring International Information Security between the Member States of the Shanghai Cooperation Organization* of 16 June 2009, and the *Arab Convention on Combating Information Technology Offences* of 21 December 2010, **53**

(Singapore)

Amend to read as follows:

(7) *Stressing* the importance of **existing international and** regional conventions on cybercrime, transnational organized crime, exchange of information and administrative assistance, including **the United Nations *Convention against Transnational Organized Crime* of 15 November 2000, the United Nations *Convention against Corruption* of 31 October 2003,** the Council of Europe *Convention on Cybercrime* of 23 November 2001 and its *Additional Protocol concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems* of 28 January 2003, the *Agreement on Cooperation in Ensuring International Information Security between the Member States of the Shanghai Cooperation Organization* of 16 June 2009, and the *Arab Convention on Combating Information Technology Offences* of 21 December 2010, **54**

(Belgium)

Amend to read as follows:

(7) *Stressing* the importance of regional conventions on cybercrime, transnational organized crime, exchange of information and administrative assistance, including the Council of Europe *Convention on Cybercrime* of 23 November 2001 and its *Additional Protocol concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems* of 28 January 2003, the *Agreement on Cooperation in Ensuring International Information Security between the Member States of the Shanghai Cooperation Organization* of 16 June 2009, and the *Arab Convention on Combating Information Technology Offences* of 21 December 2010, **as well as the Latin American and Caribbean Parliament (Parlatino) *Model Law on Cybercrime* of November 2013 and its updates, the *Model Law on Social Prevention of Violence and Crime* of November 2015, the *Model Law on Computer Crimes* of February 2021, and the *Model Law on Combating Illicit Trade and Transnational Crime* of February 2021,** **55**

(Argentina)

Amend to read as follows:

(7) *Stressing* the importance of regional conventions on cybercrime, transnational organized crime, exchange of information and administrative assistance, including the Council of Europe *Convention on Cybercrime* of 23 November 2001 and its *Additional Protocol concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems* of 28 January 2003, the *Agreement on Cooperation in Ensuring International Information Security between the Member States of the Shanghai Cooperation Organization* of 16 June 2009, ~~and~~ the *Arab Convention on Combating Information Technology Offences* of 21 December 2010, **the *Agreement on Cooperation among the Member States of the Commonwealth of Independent States in the Field of Ensuring Information Security* of 20 November 2013, and the *Agreement on Cooperation among the Member States of the Commonwealth of Independent States in the Fight Against Crimes in the Field of Information Technology* of 28 September 2018,** **56**

(Russian Federation)

Amend to read as follows:

(7) *Stressing* the importance of regional conventions on cybercrime, transnational organized crime, exchange of information, and administrative assistance, including the Council of Europe *Convention on Cybercrime* of 23 November 2001 and its *Additional Protocol concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems* of 28 January 2003, the *Agreement on Cooperation in Ensuring International Information Security between the Member States of the Shanghai Cooperation Organization* of 16 June 2009, ~~and~~ the *Arab Convention on Combating Information Technology Offences* of 21 December 2010 **and the African Union *Convention on Cyber Security and Personal Data Protection* of 27 June 2014**, **57**

(South Africa)

New preambular paragraph 7bis

(7bis) *Also stressing* that the Council of Europe *Convention on Cybercrime* of 23 November 2001 (the "Budapest Convention"), which is open for accession by any country, has become an instrument of global significance, with States Parties from, and impact in, all regions of the world, **58**

(Romania)

Preambular paragraph 8

Amend to read as follows:

(8) *Recalling* the IPU's work on the various new risks faced by our increasingly digitized societies, including the IPU resolutions *Cyber warfare: A serious threat to peace and global security* (adopted at the 132nd Assembly, Hanoi, 1 April 2015), and *Legislation worldwide to combat online child sexual exploitation and abuse* (adopted at the 143rd Assembly, Madrid, 30 November 2021),~~ which also recalls the Council of Europe Convention on the *Protection of Children against Sexual Exploitation and Sexual Abuse* (the "Lanzarote Convention") of 25 October 2007,~~ **59**

(India)

Amend to read as follows:

(8) *Recalling* the IPU's work on the various new risks faced by our increasingly digitized societies, including the IPU resolutions *Cyber warfare: A serious threat to peace and global security* (adopted at the 132nd Assembly, Hanoi, 1 April 2015), and *Legislation worldwide to combat online child sexual exploitation and abuse* (adopted at the 143rd Assembly, Madrid, 30 November 2021), which also recalls the Council of Europe Convention on the *Protection of Children against Sexual Exploitation and Sexual Abuse* (the "Lanzarote Convention") of 25 October 2007, **as well as the Latin American and Caribbean Parliament (Parlatino) *Model Law on Protection against School Violence* of November 2015, the *Model Law on guaranteeing the prevention, care and punishment of sexual abuse against children and adolescents* of November 2015, and the *Model Law against Grooming* of June 2019,** **60**

(Argentina)

New preambular paragraph 8bis

(8bis) *Noting* the principles of cybersecurity that were agreed upon in the *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* of 22 July 2015 (A/70/174) to the United Nations General Assembly, **61**

(Viet Nam)

Preambular paragraph 9

Delete the paragraph. **62**

(Belgium, Canada, Switzerland)

Amend to read as follows:

(9) ~~*Expressing concern* about the lack of universal legal instruments for the suppression of cybercrime and cyberattacks~~ ***Commending*** **the work of the United Nations on advancing responsible State behaviour in cyberspace**, **63**

(Germany)

Amend to read as follows:

(9) *Expressing concern* about the lack of universal legal instruments for the suppression of ~~cybercrime~~ **the use of information and communications technologies for criminal purposes** and ~~cyberattacks~~ **ICT threats**, **64**

(Islamic Republic of Iran)

Amend to read as follows:

(9) *Expressing concern* about the lack of universal legal instruments for the suppression of ~~cybercrime~~ **misuse of ICT for criminal purposes** and cyberattacks, **65**

(Pakistan)

Amend to read as follows:

(9) *Expressing concern* about ~~the lack of universal legal instruments~~ **the slow pace of ratification of existing legal tools** for the suppression of cybercrime ~~and cyberattacks~~**, such as the Council of Europe *Convention on Cybercrime* of 23 November 2001 and its Additional Protocols**, **66**

(Sweden)

Amend to read as follows:

(9) *Expressing concern* about the lack of universal legal instruments for the suppression of cybercrime ~~and cyberattacks~~, **67**

(Japan)

Amend to read as follows:

(9) *Expressing concern* about the lack of universal legal instruments for ~~the suppression of~~ **preventing and combating** cybercrime and ~~cyberattacks~~ **cyber incidents**, **68**

(India)

Amend to read as follows:

(9) *Expressing concern* about the lack of universal legal instruments for the suppression of cybercrime and cyberattacks, **as well as for the prevention of acts of cyberwar**, **69**

(Argentina)

Amend to read as follows:

(9) *Expressing concern* about the lack of **a** universal **strategy and** legal instruments for the suppression of cybercrime and cyberattacks, **70**

(Philippines)

Preambular paragraph 10

Delete the paragraph. **71**

(Canada)

Amend to read as follows:

(10) *Commending* the efforts of the United Nations to enact, through General Assembly resolution 74/247 of 27 December 2019, ~~a comprehensive~~ **an** international **cybercrime** convention ~~on countering the use of information and communications technologies for criminal purposes~~, and welcoming the creation of an ad hoc committee charged with drafting this convention, **72**

(Sweden)

Amend to read as follows:

(10) *Commending* the efforts of the United Nations to enact, through General Assembly resolution 74/247 of 27 December 2019, a comprehensive international convention on countering the use of information and communications technologies for criminal purposes, and welcoming the creation of an ad hoc committee charged with ~~drafting~~ **elaborating** this convention, **73**

(Singapore)

New preambular paragraph 10bis

(10bis) *Commending* also the efforts of the United Nations to convene, through United Nations General Assembly resolutions 73/27 of 5 December 2018, 75/240 of 31 December 2020 and 77/36 of 7 December 2022, an Open-ended Working Group (OEWG) on security of and in the use of information and communications technologies (ICTs), with a view to making the United Nations negotiation process on security in the use of ICTs more democratic, inclusive and transparent, **74**

(Islamic Republic of Iran)

Preambular paragraph 11

Amend to read as follows:

(11) *Welcoming* the participation of the IPU in ~~the~~ **any** multi-stakeholder consultation ~~process of that ad hoc committee~~ **that advances awareness and implementation of voluntary and non-binding norms regarding responsible State behaviour in the use of information and communications technologies,** in order to ensure that the voice of parliaments is heard, **75**

(Canada)

Amend to read as follows:

(11) *Welcoming* the participation of the IPU in the multi-stakeholder consultation process of that ad hoc committee**, as well as in the OEWG on security of and in the use of ICTs,** in order to ensure that the voice of parliaments is heard, **76**

(Islamic Republic of Iran)

Amend to read as follows:

(11) *Welcoming* the participation of the IPU in the multi-stakeholder consultation process of that ad hoc committee in order to ensure that the voice of parliaments is heard, **after consultation with the States Parties,** **77**

(Nicaragua)

Amend to read as follows:

(11) *Welcoming* the participation of the IPU in the multi-stakeholder consultation process of that ad hoc committee in order to ensure that the voice of parliaments is heard **in an effort to fight against cybercrime and cyberattacks**, **78**

(Thailand)

New preambular paragraph 11bis

(11bis) *Supporting* the Open-ended Working Group on security of and in the use of information and communications technologies 2021–2025 established pursuant to United Nations General Assembly resolution 75/240, and further *encouraging* it to take into account the outcomes of the 2010, 2013, 2015 and 2021 reports of the Groups of Governmental Experts and the 2021 report of the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security, and to add to the efforts undertaken by them, **79**

(Egypt)

New Preambular paragraph 11ter

(11ter) *Welcoming* the proposal, endorsed by the United Nations General Assembly in its resolution 77/37 of 7 December 2022, to establish a United Nations programme of action to advance responsible State behaviour in the use of information and communications technologies in the context of international security, as a permanent, inclusive, action-oriented mechanism to discuss existing and potential threats; to support States' capacities and efforts to implement and advance commitments to be guided by the framework; to promote engagement and cooperation with relevant stakeholders; and to periodically review the progress made in the implementation of the programme of action as well as the programme's future work, **80**

(Egypt)

Preambular paragraph 12

Delete the paragraph. **81**

(Canada)

Amend to read as follows:

(12) *Noting* the need for a comprehensive and global approach to ~~the issue of cybercrime and cyberattacks, including through the development of an international legal framework to address cybercrime and cyberattacks and their serious consequences for citizens and~~ **the malicious use of ICTs** to protect global peace, security and ~~economic~~ stability, **82**

(Germany)

Amend to read as follows:

(12) *Noting* the need for a ~~comprehensive and~~ global approach to the issue of cybercrime ~~and cyberattacks, including through the development of an international legal framework to address cybercrime and cyberattacks~~ and ~~their~~ **its** serious consequences for citizens**, as well as the need** to protect global peace, security and economic stability **while upholding the basic tenets of human rights including freedom of speech**, **83**

(Sweden)

Amend to read as follows:

(12) *Noting* the need for a comprehensive and global approach ~~to the issue of cybercrime and cyberattacks, including through the development of an international legal framework~~ to address cybercrime and cyberattacks and their serious consequences for citizens and to protect global peace, security and economic stability, **84**

(Switzerland)

Amend to read as follows:

(12) *Noting* the need for a comprehensive and global approach to the issue of ~~cybercrime~~ **the use of information and communications technologies for criminal purposes** and ~~cyberattacks~~ **ICT threats**, including through the development of ~~an~~ international**,** ~~legal framework~~ **legally binding frameworks tailored to the unique attributes of ICTs** to address ~~cybercrime~~ **the use of information and communications technologies for criminal purposes** and ~~cyberattacks~~ **ICT threats** and their serious consequences for citizens and to protect global peace, security and economic stability, **85**

(Islamic Republic of Iran)

Amend to read as follows:

(12) *Noting* the need for a comprehensive and global approach to the issue of ~~cybercrime~~ **misuse of ICT for criminal purposes** and cyberattacks, including through the development of an international legal framework to address ~~cybercrime~~ **misuse of ICT for criminal purposes** and cyberattacks and their serious consequences for citizens and to protect global peace, security and economic stability, **86**

(Pakistan)

Amend to read as follows:

(12) *Noting* the need for a comprehensive and global approach to the issue of cybercrime ~~and cyberattacks~~, including through the development of an international legal framework to address cybercrime ~~and cyberattacks~~ and their serious consequences for citizens and to protect global peace, security and economic stability, **87**

(Japan)

Amend to read as follows:

(12) *Noting* the need for a comprehensive and global approach to the issue of cybercrime and ~~cyberattacks~~ **cyber incidents**, including through the development of an international legal framework to address cybercrime and cyberattacks and their serious consequences for citizens and to protect global peace, security and economic stability, **88**

(India)

Amend to read as follows:

(12) *Noting* the need for a comprehensive and global approach to the issue of cybercrime and cyberattacks, including through the development of an international legal framework to address cybercrime and cyberattacks and their serious consequences for citizens **and infrastructure,** and to protect global peace, security and economic stability, **89**

(Lithuania)

New preambular paragraph 12bis

(12bis) *Noting* also that international community needs to take a comprehensive approach to threats in the sphere of ICT security that addresses not only the technological dimension of threats in this area, but also their political and ideological dimension, which includes, inter alia, the use of ICTs to interfere in the internal affairs of other States and to undermine their political, economic and social stability, **90**

(Islamic Republic of Iran)

(12bis) *Welcoming* the ongoing efforts to adapt and apply existing international legal regimes to the regulation of cyberspace, including the development of the *Tallinn Manual on the International Law Applicable to Cyber Warfare*, **91**

(Ukraine)

Preambular paragraph 13

Amend to read as follows:

(13) *Recognizing* the urgent need for legislators and governments to take more proactive national steps to combat ~~cybercrime~~ **the use of information and communications technologies for criminal purposes** and ~~cyberattacks~~ **ICT threats**, given their renewed intensity and rapidly evolving nature, **92**

(Islamic Republic of Iran)

Amend to read as follows:

(13) *Recognizing* the urgent need for legislators and governments to take more proactive national steps to combat cybercrime ~~and cyberattacks~~, given ~~their~~ **its** renewed intensity and rapidly evolving nature, **93**

(Czech Republic, Sweden)

Amend to read as follows:

(13) *Recognizing* the urgent need for legislators and governments to take more proactive national steps to combat cybercrime and ~~cyberattacks~~ **cyber incidents**, given their renewed ~~intensity~~ **severity** and rapidly evolving nature, **94**

(India)

Amend to read as follows:

(13) *Recognizing* the urgent need for legislators and governments to take more proactive national steps to combat ~~cybercrime~~ **misuse of ICT for criminal purposes** and cyberattacks, given their renewed intensity and rapidly evolving nature, **95**

(Pakistan)

Amend to read as follows:

(13) *Recognizing* the urgent need for legislators ~~and~~**,** governments **and all stakeholders** to take more proactive national steps to combat cybercrime and cyberattacks, given their renewed intensity and rapidly evolving nature, **96**

(Thailand)

Amend to read as follows:

(13) *Recognizing* the urgent need for legislators and governments to take more proactive national steps to combat cybercrime and cyberattacks, given their renewed intensity and rapidly evolving nature, **while fully respecting human rights, fundamental freedoms and the rule of law, as well as their obligations under international human rights law,** **97**

(Canada)

Amend to read as follows:

(13) *Recognizing* the urgent need for legislators and governments to take more proactive national steps to combat cybercrime and cyberattacks, given their renewed intensity and rapidly evolving nature, **and equally to reinforce protections for freedom of expression and other fundamental rights**, **98**

(South Africa)

New preambular paragraph 13bis

(13bis) *Recognizing* that all actions in this field need to have respect for human rights and fundamental rights at their centre, **99**

(Sweden)

(13bis) *Noting* the uneven development in countries' IT application capacity and ability to protect IT infrastructure, and *emphasizing* the need for increased technical assistance and collaboration, especially for developing countries, **100**

(Viet Nam)

New preambular paragraph 13ter

(13ter) *Noting* that States shall act in accordance with their obligations under international human rights law, including but not limited to the *International Covenant on Civil and Political Rights*, the *Convention on the Rights of the Child*, the *Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment*, the *Convention on the Elimination of All Forms of Discrimination against Women*, and additional protocols and other relevant international human rights instruments, **101**

(Sweden)

Preambular paragraph 14

Delete the paragraph. **102**

(India)

Amend to read as follows:

(14) *Recognizing also* the need for common, international parliamentary action to ~~provide a protective shield for citizens, governments and States, which are all stakeholders in this task,~~ **advance awareness and implementation of voluntary and non-binding norms regarding responsible State behaviour in the use of information and communications technologies,** **103**

(Canada)

Amend to read as follows:

(14) *Recognizing also* the need for common, **regional and** international parliamentary action to provide a protective shield for citizens, governments and States, which are all stakeholders in this task, **as well as for the necessary legislative coordination at the subnational level,** **104**

(Argentina)

New preambular paragraph 14bis

(14bis) *Noting* that cybercrime may constitute a serious threat to democratic processes, notably interference in elections through cybersecurity breaches or false social media accounts, **105**

(Finland)

(14bis) *Recalling* the damaging impacts of unilateral coercive measures and other restrictions during the COVID-19 pandemic, which have been widely acknowledged, including in United Nations reports, **106**

(Islamic Republic of Iran)

New preambular paragraph 14ter

(14ter) *Urging* parliaments to call upon their governments to refrain from promulgating or applying any unilateral coercive measures (unilateral financial, economic or trade measures) that impede or negatively affect the ability of States to prevent and combat cybercrime or to render cooperation and assistance to each other in that regard, **107**

(Islamic Republic of Iran)

Preambular paragraph 15

Amend to read as follows:

(15) *Acknowledging* that women~~, young people and children are the most vulnerable and suffer the greatest aggressions on the internet, and are personally, socially, culturally and economically affected by cybercriminals~~ **and girls, the elderly and children, among others, are most at risk of being exposed to threats in cyberspace**, **108**

(Germany)

Amend to read as follows:

(15) *Acknowledging* that women, young people, **elderly people, disabled persons** and children are ~~the most~~ **particularly** vulnerable and suffer the greatest **number of** aggressions on the internet,~~ and are personally, socially, culturally and economically affected by cybercriminals.~~ **109**

(Belgium)

Amend to read as follows:

(15) *Acknowledging* that women~~, young people~~ and children, **as well as elderly people,** are the most vulnerable and suffer the greatest aggressions on the internet, and are personally, socially, culturally and economically affected by ~~cybercriminals~~ **cybercrimes**, **110**

(Czech Republic)

Amend to read as follows:

(15) *Acknowledging* that women, young people and children are the most vulnerable and suffer the greatest aggressions ~~on the internet~~ **in cyberspace**, and are personally, socially, culturally and economically affected by cybercriminals, **111**

(Lithuania)

Amend to read as follows:

(15) *Acknowledging* that women, young people and children are the most vulnerable and suffer the greatest aggressions on the internet, and are personally, socially, culturally and economically affected by cybercriminals, **while *emphasizing* the need to increase cooperation with the private sector and service providers in order to protect those affected,** **112**

(Thailand)

Amend to read as follows:

(15) *Acknowledging* that women, young people**,** ~~and~~ children **and racialized communities** are the most vulnerable and suffer the greatest aggressions on the internet, and are personally, socially, culturally and economically affected by cybercriminals, **113**

(Canada)

Amend to read as follows:

(15) *Acknowledging* that women, young people and children**, and persons with disabilities** are the most vulnerable and suffer the greatest aggressions on the internet, and are personally, socially, culturally and economically affected by cybercriminals, **114**

(Finland)

Amend to read as follows:

(15) *Acknowledging* that women, young **and elderly** people**,** and children are the most vulnerable and suffer the greatest aggressions on the internet, and are personally, socially, culturally and economically affected by cybercriminals, **115**

(Viet Nam)

Amend to read as follows:

(15) *Acknowledging* that women, young people**, the elderly** and children are the most vulnerable and suffer the greatest aggressions on the internet, and are personally, socially, culturally and economically affected by cybercriminals, **116**

(Türkiye)

New preambular paragraph 15bis

(15bis) *Bearing in mind* that research shows that, in times of COVID-19, more women and girls have become victims of online violence through physical threats, sexual harassment and stalking, among others, **117**

(Philippines)

(15bis) *Acknowledging* the need for efforts to promote gender equality and the empowerment of women and girls in all their diversity, including through gender mainstreaming, in the development, implementation and application of policies, programmes and legislation in this field, **118**

(Sweden)

Preambular paragraph 16

Amend to read as follows:

(16) *Noting* the nature of the threats and risks of **the** transnational ~~cybercrime~~ **use of information and communications technologies for criminal purposes** and ~~cyberattacks~~ **ICT threats** to international peace and security, and the tremendous developments in ~~cyberspace~~ **the ICT environment**, as a result of which the methods used by cybercriminals **and malicious actors** are becoming increasingly sophisticated, **119**

(Islamic Republic of Iran)

Amend to read as follows:

(16) *Noting* the nature of the threats and risks of transnational ~~cybercrime~~ **misuse of ICT for criminal purposes** and cyberattacks to international peace and security, and the tremendous developments in cyberspace, as a result of which the methods used by cybercriminals are becoming increasingly sophisticated, **120**

(Pakistan)

Amend to read as follows:

(16) *Noting* the nature of the threats and risks of transnational cybercrime ~~and cyberattacks~~ to international peace and security, and the tremendous developments in cyberspace, as a result of which the methods used by cybercriminals are becoming increasingly sophisticated, **121**

(Sweden)

Amend to read as follows:

(16) *Noting* the nature of the threats and risks of transnational cybercrime and ~~cyberattacks~~ **cyber incidents** to international peace and security, and the tremendous developments in cyberspace, as a result of which the methods used by cybercriminals are becoming increasingly sophisticated, **122**

(India)

Amend to read as follows:

(16) *Noting* the nature of the threats and risks of transnational cybercrime and **malicious** cyberattacks to international peace and security, and the tremendous developments in cyberspace, as a result of which the methods used by cybercriminals are becoming increasingly sophisticated, **123**

(Belgium)

New preambular paragraph 16bis

(16bis) *Expressing concern* about the indiscriminate use of cyberattacks against objects of civilian infrastructure, which cause disproportionate and unnecessary damage to energy generation and distribution facilities, hospitals, bank systems and other critical national infrastructure, **124**

(Ukraine)

Preambular paragraph 17

Amend to read as follows:

(17) *Noting also* that cybercrime ~~and cyberattacks encompass~~ not only **encompasses** attacks on ~~information and communications technologies (ICTs)~~ **computer systems**, breaches of privacy, and the creation and deployment of malware, but **is** also ~~attacks~~ **increasingly facilitating cyberattacks** on critical ~~national~~ **civilian** infrastructure, as well as other acts that can occur offline and be facilitated by ~~ICTs~~ **computer systems**, including online fraud, drug purchases, money-laundering, hate crimes, ~~propaganda, extremist indoctrination,~~ and the sexual exploitation of women and children via the internet – all of which negatively affect global security and economic stability, **125**

(Sweden)

Amend to read as follows:

(17) *Noting also* that cybercrime and cyberattacks encompass ~~not only~~ **in particular** attacks on information and communications technologies (ICTs), breaches of privacy, and the creation and deployment of malware, ~~but also attacks on critical national infrastructure, as well as other acts that can occur offline and be facilitated by ICTs, including online fraud, drug purchases, money-laundering, hate crimes, propaganda, extremist indoctrination, and the sexual exploitation of women and children via the internet – all of which negatively affect global security and economic stability~~ **while also acknowledging the need for international cooperation on other serious crimes that can be facilitated by ICTs**, **126**

(Germany)

Amend to read as follows:

(17) *Noting also* that ~~cybercrime~~ **the use of information and communications technologies for criminal purposes** and ~~cyberattacks~~ **ICT threats** encompass not only attacks on information and communications technologies (ICTs), breaches of privacy, **disinformation campaigns, fabricated image-building, xenophobia, interference in the internal affairs of States,** and the creation and deployment of malware, but also attacks on critical national infrastructure, as well as other acts that can occur offline and be facilitated by ICTs, including online fraud, drug purchases, money-laundering, hate crimes, propaganda, extremist indoctrination, and the sexual exploitation of women and children via the internet – all of which negatively affect global security**, as well as** economic **and cultural** stability, **127**

(Islamic Republic of Iran)

Amend to read as follows:

(17) *Noting also* that cybercrime and ~~cyberattacks~~ **cyber incidents** encompass not only attacks on information and communications technologies (ICTs), breaches of privacy, and the creation and deployment of malware, but also attacks on critical national infrastructure, as well as other acts that can occur offline and be facilitated by ICTs, including online fraud, drug purchases, money-laundering, hate crimes, propaganda, extremist indoctrination, and the sexual exploitation of women and children via the internet – all of which negatively affect global security and economic stability, **128**

(India)

Amend to read as follows:

(17) *Noting also* that ~~cybercrime~~ **misuse of ICT for criminal purposes** and cyberattacks encompass not only attacks on information and communications technologies (ICTs), breaches of privacy, and the creation and deployment of malware, but also attacks on critical national infrastructure, as well as other acts that can occur offline and be facilitated by ICTs, including online fraud, drug purchases, money-laundering, hate crimes, propaganda, extremist indoctrination, and the sexual exploitation of women and children via the internet – all of which negatively affect global security and economic stability, **129**

(Pakistan)

Amend to read as follows:

(17) *Noting also* that cybercrime and cyberattacks encompass not only attacks on ~~information and communications technologies (ICTs)~~ **computer systems**, breaches of privacy, and the creation and deployment of malware, but also attacks on critical national infrastructure, as well as other acts that can occur offline ~~and be facilitated by ICTs~~ **but that now take place in cyberspace with the facilitation of computer systems**, including online fraud, drug purchases, money-laundering, hate crimes, propaganda, extremist indoctrination, and the sexual exploitation of women and children via the internet – all of which negatively affect global security and economic stability, **130**

(Singapore)

Amend to read as follows:

(17) *Noting also* that cybercrime and cyberattacks ~~encompass not only~~ **include but are not limited to** attacks on information and communications technologies (ICTs), breaches of privacy, ~~and~~ the creation and deployment of malware, ~~but also~~ **and** attacks on critical national infrastructure, as well as other acts that can occur offline and be facilitated by ICTs, including online fraud, drug purchases, money-laundering, hate crimes, propaganda, extremist indoctrination, and the sexual exploitation of women and children via the internet – all of which negatively affect global security and economic stability, **131**

(Canada)

Amend to read as follows:

(17) *Noting also* that cybercrime and cyberattacks encompass not only attacks on information and communications technologies (ICTs), breaches of privacy, and the creation and deployment of malware, but also attacks on critical national infrastructure, as well as other acts that can occur offline and be facilitated by ICTs, including online fraud, drug purchases, money-laundering, ~~hate crimes, propaganda, extremist indoctrination,~~ and the sexual exploitation of women and children via the internet – all of which negatively affect global security and economic stability, **132**

(Belgium)

Amend to read as follows:

(17) *Noting also* that cybercrime and cyberattacks encompass not only attacks on information and communications technologies (ICTs), breaches of privacy, and the creation and deployment of malware, but also attacks on critical national infrastructure, as well as other acts that can occur offline and be facilitated by ICTs, including online fraud, drug purchases, money-laundering, hate crimes, propaganda, extremist indoctrination, **cyberbullying and stalking, trafficking in persons,** and the sexual exploitation of women and children via the internet – all of which negatively affect global security and economic stability, **133**

(South Africa)

Amend to read as follows:

(17) *Noting also* that cybercrime and cyberattacks encompass not only attacks on information and communications technologies (ICTs), breaches of privacy, and the creation and deployment of malware, but also attacks on critical national infrastructure, as well as other acts that can occur offline and be facilitated by ICTs, including online fraud, drug purchases, money-laundering, **human trafficking,** hate crimes, propaganda, extremist indoctrination, and the sexual exploitation of women and children via the internet – all of which negatively affect global security and economic stability, **134**

(Romania)

Amend to read as follows:

(17) *Noting also* that cybercrime and cyberattacks encompass not only attacks on information and communications technologies (ICTs), breaches of privacy, and the creation and deployment of malware, but also attacks on critical national infrastructure, as well as other acts that can occur offline and be facilitated by ICTs, including online fraud, drug purchases, money-laundering, hate crimes, propaganda, extremist indoctrination, and the sexual exploitation**, especially** of women and children**,** via the internet – all of which negatively affect global security and economic stability, **135**

(Lithuania)

New preambular paragraph 17bis

(17bis) *Acknowledging* the value of exchanging experiences with different definitions of cybercrime and cyberattacks in order to build a broader foundation for developing confidence-building measures, **136**

(Canada)

(17bis) *Recognizing* that the lack of responsibility of service providers and transnational platforms also poses a serious threat in the field of ICTs, which needs to be addressed by the international community, **137**

(Islamic Republic of Iran)

Preambular paragraph 18

Delete the paragraph. **138**

(Japan)

Amend to read as follows:

(18) *Considering* that most national laws were enacted ~~long~~ before cybercrime ~~and cyberattacks~~ arose and therefore do not always adequately address these threats, **139**

(Czech Republic)

Amend to read as follows:

(18) *Considering* that most national laws were enacted long before cybercrime ~~and cyberattacks~~ arose and therefore do not always adequately address these threats, **140**

(Sweden)

Amend to read as follows:

(18) *Considering* that most national laws were enacted long before ~~cybercrime~~ **the use of information and communications technologies for criminal purposes** and ~~cyberattacks~~ **ICT threats** arose and therefore do not always adequately address these threats, **141**

(Islamic Republic of Iran)

Amend to read as follows:

(18) *Considering* that most national laws were enacted long before ~~cybercrime~~ **misuse of ICT for criminal purposes** and cyberattacks arose and therefore do not always adequately address these threats, **142**

(Pakistan)

Amend to read as follows:

(18) *Considering* that most national laws were enacted long before **the spread of** cybercrime and cyberattacks ~~arose~~ and therefore do not always adequately address these threats, **143**

(Thailand)

Amend to read as follows:

(18) *Considering* that most national laws were enacted long before cybercrime and **malicious** cyberattacks arose and therefore do not always adequately address these threats, **144**

(Belgium)

New preambular paragraph 18bis

Amend to read as follows:

(18bis) *Stressing* the need for enhanced efforts to close the digital divide by facilitating the transfer of information technology and capacity-building to developing countries in the areas of the use of information and communications technologies for criminal purposes and ICT security, **145**

(Islamic Republic of Iran)

OPERATIVE PART

Operative paragraph 1

Delete the paragraph. **146**

(Belgium, Canada, Japan, Switzerland)

Amend to read as follows:

1. *Calls upon* the international community, through the United Nations, to **adapt and** adopt **a** common global ~~definitions~~ **definition** of cybercrime ~~and cyberattacks that include every variation of such acts and the acts they may facilitate~~; **147**

(Sweden)

Amend to read as follows:

1. *Calls upon* the international community, through the United Nations, to adopt common global definitions of cybercrime and cyberattacks ~~that include every variation of such acts and the acts they may facilitate~~; **148**

(Germany, Republic of Korea, Singapore)

Amend to read as follows:

1. *Calls upon* the international community, through the United Nations, to adopt **a** common global ~~definitions~~ **definition** of cybercrime ~~and cyberattacks~~ that ~~include~~ **includes** every variation of such ~~acts~~ **act** and the acts ~~they~~ **it** may facilitate**, including a clear differentiation between cybercrime and cyberwar, and between cybersecurity and cyberdefence**; **149**

(Argentina)

Amend to read as follows:

1. *Calls upon* the international community, through the United Nations, to adopt **a** common global ~~definitions~~ **definition** of cybercrime ~~and cyberattacks~~ that ~~include~~ **includes** every variation of such acts and the acts they may facilitate; **150**

(Czech Republic)

Amend to read as follows:

1. *Calls upon* the international community, through the United Nations, to adopt common**,** global**,** ~~definitions of cybercrime and cyberattacks~~ **universal terminology in the field of ICT security** that ~~include~~ **includes** every variation of such acts and the acts they may facilitate; **151**

(Islamic Republic of Iran)

Amend to read as follows:

1. *Calls upon* the international community, through the United Nations, to adopt common global definitions of ~~cybercrime~~ **crimes committed with the use of ICTs** and ~~cyberattacks~~ **cyber incidents** that include every variation of such acts and the acts they may facilitate; **152**

(India)

Amend to read as follows:

1. *Calls upon* the international community, through the United Nations, to adopt common global definitions of ~~cybercrime~~ **misuse of ICT for criminal purposes** and cyberattacks that include every variation of such acts and the acts they may facilitate; **153**

(Pakistan)

Amend to read as follows:

1. *Calls upon* the international community, through the United Nations, to adopt common global definitions of cybercrime and cyberattacks that include every variation of such acts and the acts they may facilitate**, taking into account the realities of each nation**; **154**

(Nicaragua)

Operative paragraph 2

Delete the paragraph. **155**

(Belgium, Canada)

Amend to read as follows:

2. *Encourages* parliaments to call upon their governments to support the efforts of the United Nations to enact a ~~new~~ **comprehensive international** convention on ~~cybercrime~~ **countering the use of information and communications technologies for criminal purposes** by participating actively in its drafting; **156**

(India, Russian Federation)

Amend to read as follows:

2. *Encourages* parliaments to call upon their governments to support the efforts of the United Nations to enact a new convention on ~~cybercrime~~ **the use of information and communications technologies for criminal purposes** by participating actively in its drafting; **157**

(Islamic Republic of Iran)

Amend to read as follows:

2. *Encourages* parliaments to call upon their governments to support the efforts of the United Nations to enact a new convention on ~~cybercrime~~ **misuse of ICT for criminal purposes** by participating actively in its drafting; **158**

(Pakistan)

New operative paragraph 2bis

2bis. *Also encourages* parliaments to call upon their governments to support the efforts of the United Nations OEWG on security of and in the use of information and communications technologies (ICTs) by participating actively in its sessions; **159**

(Islamic Republic of Iran)

Operative paragraph 3

Delete the paragraph. **160**

(Belgium, Canada)

Amend to read as follows:

3. *Urges* parliaments and their governments to convey the need to include, in the convention, ~~comprehensive definitions of cybercrime and cyberattacks, along with~~ mechanisms supporting international cooperation to combat cybercrime ~~and cyberattacks,~~ **with adequate safeguards**; **161**

(Sweden)

Amend to read as follows:

3. *Urges* parliaments and their governments to convey the need to include, in the convention, ~~comprehensive definitions of cybercrime and cyberattacks, along with~~ mechanisms supporting international cooperation to combat cybercrime ~~and cyberattacks~~; **162**

(Japan)

Amend to read as follows:

3. *Urges* parliaments and their governments to convey the need to include, in the convention, ~~comprehensive definitions of cybercrime and cyberattacks, along with~~ mechanisms supporting international cooperation to combat cybercrime and cyberattacks; **163**

(Lithuania, Republic of Korea)

Amend to read as follows:

3. *Urges* parliaments and their governments to convey the need to include, in the convention, **a** comprehensive ~~definitions of cybercrime and cyberattacks~~ **catalogue of clearly defined cybercrimes**, along with mechanisms supporting international cooperation to combat cybercrime and cyberattacks; **164**

(Switzerland)

Amend to read as follows:

3. *Urges* parliaments and their governments to convey the need to include, in the convention, **a** comprehensive ~~definitions~~ **definition** of cybercrime ~~and cyberattacks~~, along with mechanisms supporting international cooperation to combat **such crime** ~~cybercrime and cyberattacks~~**, without prejudice to the application of current national legislation on cybersecurity and the protection of personal data**; **165**

(Argentina)

Amend to read as follows:

3. *Urges* parliaments and their governments to convey the need to include, in the convention, comprehensive definitions of cybercrime ~~and cyberattacks~~, along with mechanisms supporting international cooperation to combat cybercrime ~~and cyberattacks~~; **166**

(Germany)

Amend to read as follows:

3. *Urges* parliaments and their governments to convey the need to include, in the convention**,** ~~comprehensive definitions of cybercrime and cyberattacks~~ **as well as the outcomes of the OEWG on ICT security, universal terminology in the field of ICT security**, along with mechanisms supporting international cooperation to combat ~~cybercrime~~ **the use of information and communications technologies for criminal purposes** and ~~cyberattacks~~ **ICT threats**; **167**

(Islamic Republic of Iran)

Amend to read as follows:

3. *Urges* parliaments and their governments to convey the need to include, in the convention, comprehensive definitions of ~~cybercrime~~ **crimes committed with the use of ICTs** and ~~cyberattacks~~ **cyber incidents**, along with mechanisms supporting international cooperation to combat cybercrime and ~~cyberattacks~~ **cyber incidents**; **168**

(India)

Amend to read as follows:

3. *Urges* parliaments and their governments to convey the need to include, in the convention, comprehensive definitions of ~~cybercrime~~ **misuse of ICT for criminal purposes** and cyberattacks, along with mechanisms supporting international cooperation to combat ~~cybercrime~~ **misuse of ICT for criminal purposes** and cyberattacks; **169**

(Pakistan)

Amend to read as follows:

3. *Urges* parliaments and their governments to convey the need to include, in the convention, comprehensive definitions of cybercrime and cyberattacks **including related criminal offences**, **and safeguards required to protect human rights and fundamental freedoms**, along with mechanisms supporting international cooperation **and technical assistance** to combat **and prevent** cybercrime and cyberattacks; **170**

(South Africa)

Amend to read as follows:

3. *Urges* parliaments and their governments to convey the need to include, in the convention, comprehensive definitions of cybercrime and cyberattacks, along with mechanisms supporting international **and multi-stakeholder** cooperation**, as well as their guidelines for implementation and evaluation,** to **effectively** combat cybercrime and cyberattacks; **171**

(Thailand)

New operative paragraph 3bis

3bis. *Also urges* parliaments and their governments to ensure that the new convention complements existing international and regional instruments on cybercrime and on transnational organized crime, as well as other relevant instruments, in particular those relating to the protection of human rights; **172**

(Romania)

3bis. *Also urges* parliaments and their governments to emphasize the importance of including strong protection of human rights and fundamental freedoms in the new convention; **173**

(Sweden)

Operative paragraph 4

Delete the paragraph. **174**

(Belgium, Canada)

Amend to read as follows:

4. *Invites* parliaments and their governments to use this convention, once adopted, as a means to strengthen national legislation and to increase international cooperation to combat cybercrime ~~and cyberattacks~~; **175**

(Argentina, Czech Republic, Germany, Sweden)

Amend to read as follows:

4. *Invites* parliaments and their governments to use this convention, once adopted, as a means to strengthen national legislation and to increase international cooperation to combat ~~cybercrime~~ **the use of information and communications technologies for criminal purposes** and ~~cyberattacks~~ **ICT threats**; **176**

(Islamic Republic of Iran)

Amend to read as follows:

4. *Invites* parliaments and their governments to use this convention, once adopted, as a means to strengthen national legislation and to increase international cooperation to combat ~~cybercrime~~ **misuse of ICT for criminal purposes** and cyberattacks; **177**

(Pakistan)

Amend to read as follows:

4. *Invites* parliaments and their governments to use this convention, once adopted, as a means to ~~strengthen~~ **update** national legislation and to increase international cooperation to combat cybercrime and cyberattacks; **178**

(Japan)

Amend to read as follows:

4. *Invites* parliaments and their governments to use this convention, once adopted **and in force**, as a means to strengthen national legislation and to increase international cooperation to combat cybercrime and cyberattacks; **179**

(Viet Nam)

Amend to read as follows:

4. *Invites* parliaments and their governments to use ~~this~~ **the** convention **referred to in operative paragraphs 2 and 3 above**, once adopted, as a means to strengthen national legislation and to increase international cooperation to combat cybercrime and cyber attacks; **180**

(South Sudan)

New operative paragraph 4bis

4bis. *Encourages* parliaments to take full account of the disruptive and destructive potential of cyberattacks by addressing the issue of critical national infrastructure protection, including but not limited to electricity, water, gas, communication, nuclear power plants, transportation, finance and food supply; **181**

(Argentina)

4bis. *Encourages* parliaments to consider taking the necessary steps for their country to accede, if it has not yet done so, to existing international instruments that address the use of ICTs for criminal purposes, including the Council of Europe *Convention on Cybercrime* of 23 November 2001 (the "Budapest Convention"), which is the most comprehensive multilateral cybercrime treaty in force and is open for accession by all States; **182**

(Romania)

Operative paragraph 5

Amend to read as follows:

5. *Calls upon* parliaments to ~~enact new~~ **make sure their** legislation on cybercrime ~~and cyberattacks~~ **is up to date and relevant**, considering the ongoing increase in the scale and frequency of such acts and their implications for international peace and security and global economic stability; **183**

(Sweden)

Amend to read as follows:

5. *Calls upon* parliaments to enact, **where appropriate,** new legislation on cybercrime ~~and cyberattacks~~, considering the ongoing increase in the scale and frequency of such acts and their implications for international peace and security and global economic stability; **184**

(Czech Republic)

Amend to read as follows:

5. *Calls upon* parliaments to enact new legislation on ~~cybercrime~~ **the use of information and communications technologies for criminal purposes** and ~~cyberattacks~~ **ICT threats**, considering the ongoing increase in the scale and frequency of such acts and their implications for international peace and security and global economic stability; **185**

(Islamic Republic of Iran)

Amend to read as follows:

5. *Calls upon* parliaments to enact new legislation on cybercrime and ~~cyberattacks~~ **cybersecurity**, considering the ongoing increase in the scale and frequency of ~~such acts~~ **cybercrime and malicious cyberattacks** and their implications for international peace and security and global economic stability; **186**

(Belgium)

Amend to read as follows:

5. *Calls upon* parliaments to enact new legislation on ~~cybercrime~~ **misuse of ICT for criminal purposes** and cyberattacks, considering the ongoing increase in the scale and frequency of such acts and their implications for international peace and security and global economic stability; **187**

(Pakistan)

Amend to read as follows:

5. *Calls upon* parliaments to ~~enact new~~ **update national** legislation on cybercrime and cyberattacks, considering the ongoing increase in the scale and frequency of such acts and their implications for international peace and security and global economic stability; **188**

(Japan)

Amend to read as follows:

5. *Calls upon* parliaments ~~to enact~~ **that have yet to enact a** new ~~legislation~~ **law** on cybercrime and cyberattacks **to do so**, considering the ongoing increase in the scale and frequency ~~of such~~ **of commission of these illicit** acts and their **high-risk** implications for international peace and security and global economic stability; **189**

(Nicaragua)

Amend to read as follows:

5. *Calls upon* parliaments to enact new legislation on cybercrime and cyberattacks **in accordance with international law, including international human rights instruments**, considering the ongoing increase in the scale and frequency of such acts and their implications for international peace and security and global economic stability**, and to include in such legislation extraterritorial jurisdiction to enable the prosecution of criminal acts, irrespective of where those acts were committed and whether they constitute offences in the foreign jurisdiction**; **190**

(South Africa)

Amend to read as follows:

5. *Calls upon* parliaments to enact new legislation on cybercrime and cyberattacks**, by engaging all stakeholders, including the private sector, academia, civil society and the technical community**, considering the ongoing increase in the scale and frequency of such acts and their implications for **national security,** international peace and security**,** and global economic stability; **191**

(Romania)

Amend to read as follows:

5. *Calls upon* parliaments to enact new legislation or **revise laws** on cybercrime and cyberattacks, considering the ongoing increase in the scale and frequency of such acts and their implications for international peace and security and global economic stability; **192**

(Viet Nam)

Amend to read as follows:

5. *Calls upon* parliaments to enact new legislation on cybercrime and cyberattacks, **and to allocate the necessary resources to this end**, considering the ongoing increase in the scale and frequency of such acts and their implications for international peace and security and global economic stability; **193**

(France)

Amend to read as follows:

5. *Calls upon* parliaments to enact new legislation on cybercrime and cyberattacks, considering the ongoing increase in the scale**, scope, speed, complexity** and frequency of such acts and their implications for international peace and security and global economic stability; **194**

(India)

New operative paragraph 5bis

5bis. *Also calls upon* the international community not to use information and communications technologies and information and communications networks to interfere in the internal affairs of other States or with the aim of undermining their political, economic and social stability; **195**

(Islamic Republic of Iran)

5bis. *Urges* parliaments to ensure that human rights impact assessments are embedded in all legislative processes on cybercrime and cyberattacks; **196**

(Romania)

5bis. *Also calls upon* parliaments to enhance the capacity of law enforcement officers, including investigative authorities, prosecutors and judges, in the field of cyberattacks and cybercrime, and to equip them to effectively investigate, prosecute and adjudicate cases of cyberattacks and cybercrime offences; **197**

(South Africa)

5bis. *Urges* parliaments and governments to devise and adopt a universal legal framework for cyberwarfare, incorporating the concepts of distinction and proportionality, to prevent cyberattacks against critical civilian infrastructure; **198**

(Ukraine)

Operative paragraph 6

Amend to read as follows:

6. *Encourages* parliaments to make full use of their oversight function to ensure that governments have the tools to control the rapid increase in ~~cybercrime and cyberattacks~~ **cybercrimes** and to protect the ~~digital security~~ **cybersecurity**, identity, privacy and data of citizens, especially the most vulnerable; **199**

(Czech Republic)

Amend to read as follows:

6. *Encourages* parliaments to make full use of their oversight function to ensure that governments have the tools to ~~control~~ **prevent and combat** the rapid increase in cybercrime ~~and cyberattacks~~ and to protect the digital security, identity, privacy and data of citizens, especially the most vulnerable; **200**

(Belgium)

Amend to read as follows:

6. *Encourages* parliaments to make full use of their oversight function to ensure that governments have the tools to control the rapid increase in cybercrime ~~and cyberattacks~~ and to protect the digital security, identity, privacy and data of citizens, especially the most vulnerable**, while safeguarding human rights and freedoms**; **201**

(Sweden)

Amend to read as follows:

6. *Encourages* parliaments to make full use of their oversight function to ensure that governments have the tools to control the rapid increase in ~~cybercrime~~ **the use of information and communications technologies for criminal purposes** and ~~cyberattacks~~ **ICT threats** and to protect the digital security, identity, privacy and data of citizens, especially the most vulnerable; **202**

(Islamic Republic of Iran)

Amend to read as follows:

6. *Encourages* parliaments to make full use of their oversight function to ensure that governments have the tools to control the rapid increase in ~~cybercrime~~ **misuse of ICT for criminal purposes** and cyberattacks and to protect the digital security, identity, privacy and data of citizens, especially the most vulnerable; **203**

(Pakistan)

Amend to read as follows:

6. *Encourages* parliaments to make full use of their ~~oversight~~ function to ensure that governments have the tools ~~to control~~ **against** the rapid increase in cybercrime and cyberattacks and to protect the digital security, identity, privacy and data of citizens, especially the most vulnerable; **204**

(Japan)

Amend to read as follows:

6. *Encourages* parliaments to make full use of their oversight function to ensure that governments have the tools to control the rapid increase in cybercrime and cyberattacks and to protect the digital security, identity, privacy and data of citizens~~, especially the most vulnerable~~; **205**

(India)

Amend to read as follows:

6. *Encourages* parliaments to make full use of their oversight function to ensure that governments have the tools, **including appropriate resources and capacity,** to control the rapid increase in cybercrime and cyberattacks and to protect the digital security, identity, privacy and data of citizens, especially the most vulnerable; **206**

(South Africa)

Amend to read as follows:

6. *Encourages* parliaments to make full use of their oversight function to ensure that governments have the tools to control the rapid increase in cybercrime and cyberattacks and to protect **human rights in cyberspace, including** the digital security, identity, privacy and data of citizens, especially the most vulnerable; **207**

(Argentina)

New operative paragraph 6bis

6bis. *Calls upon* parliaments and governments of developed countries to assist developing countries in their efforts to enhance capacity-building on ICT security and to close the digital divide; **208**

(Islamic Republic of Iran)

New operative paragraph 6ter

6ter. *Also calls upon* parliaments and their governments to refrain from adopting any unilateral coercive measures that restrict or prevent universal access to the benefits of ICTs; **209**

(Islamic Republic of Iran)

Operative paragraph 7

Amend to read as follows:

7. *Strongly recommends* that parliaments **ensure that their national legislative framework on the protection of critical national infrastructure, including the infrastructure that supports the internet, is up to date, and that they review or** establish legislative frameworks ~~aimed at protecting the infrastructure that supports the internet, in particular submarine cables, satellite networks and critical internet services, as well as large public and private data centres providing cloud services, which in turn should exchange information on cyber incidents, in real time, through relevant national and supranational bodies~~ **where necessary**; **210**

(Switzerland)

Amend to read as follows:

7. *Strongly recommends* that parliaments establish legislative frameworks aimed at protecting ~~the~~ **critical civilian** infrastructure ~~that supports the internet, in particular submarine cables, satellite networks and critical internet services, as well as large public and private data centres providing cloud services~~, which in turn should exchange information on cyber incidents, in real time, through relevant national and supranational bodies; **211**

(Sweden)

Amend to read as follows:

7. *Strongly recommends* that parliaments establish legislative frameworks aimed at protecting the infrastructure that supports the internet, in particular submarine cables, satellite networks and critical internet services, ~~as well as large public and private data centres providing cloud services, which in turn should exchange information on cyber incidents, in real time, through relevant national and supranational bodies~~ **and at facilitating collaboration with the private sector**; **212**

(Germany)

Amend to read as follows:

7. *Strongly recommends* that parliaments establish legislative frameworks ~~aimed at protecting~~ **for internet service providers, in order to protect** the infrastructure that supports the internet, in particular submarine cables, satellite networks and critical internet services, as well as large public and private data centres providing cloud services, which in turn should exchange information on cyber incidents, in real time, through relevant national and supranational bodies; **213**

(Nicaragua)

Amend to read as follows:

7. *Strongly recommends* that parliaments establish legislative frameworks aimed at protecting the infrastructure that supports the internet, in particular submarine cables, satellite networks and critical internet services, as well as large public and private data centres providing cloud services, which in turn should exchange information on cyber incidents, in real time, through relevant national and ~~supranational~~ **international** bodies; **214**

(India)

Amend to read as follows:

7. *Strongly recommends* that parliaments establish legislative frameworks aimed at protecting the infrastructure that supports the internet, in particular submarine cables, satellite networks and critical internet services, as well as large public and private data centres providing cloud services, which in turn should exchange information on cyber incidents~~, in real time,~~ through relevant national and supranational bodies; **215**

(Belgium)

Amend to read as follows:

7. *Strongly recommends* that parliaments establish legislative frameworks aimed at protecting the infrastructure that supports ~~the internet~~ **cyberspace**, in particular submarine cables, satellite networks and critical internet services, as well as large public and private data centres providing cloud services, which in turn should exchange information on cyber incidents, in real time, through relevant national and supranational bodies; **216**

(Lithuania)

Amend to read as follows:

7. *Strongly recommends* that parliaments establish legislative frameworks aimed at protecting **from cyberattacks** the infrastructure that supports the internet, in particular submarine cables, satellite networks and critical internet services, as well as large public and private data centres providing cloud services, which in turn should exchange information on cyber incidents, in real time, through relevant national and supranational bodies; **217**

(Argentina)

New operative paragraph 7bis

7bis. ***Also recommends*** **that all States play the same role in, and carry equal responsibility for, international governance of the internet through the establishment of a multilateral, transparent and democratic international internet governance mechanism;** **218**

(Islamic Republic of Iran)

Operative paragraph 8

Amend to read as follows:

8. *Encourages* parliaments to promote a secure ~~cyberspace~~ **ICT environment** by calling on their governments to cooperate in stopping ~~cybercrime~~ **the use of information and communications technologies for criminal purposes**, ~~and~~ **as well as** cybercriminals **and malicious actors**, to respond to requests for assistance **and capacity-building**, if possible in real time, to secure the supply chain of companies in their countries, to report **voluntarily** on potential vulnerabilities to third parties to assist them in preventing future incidents, and in particular to support and protect all cyber incident response teams within and beyond their borders; **219**

(Islamic Republic of Iran)

Amend to read as follows:

8. *Encourages* parliaments to promote a secure cyberspace by calling on their governments to cooperate in stopping ~~cybercrime~~ **misuse of ICT for criminal purposes** and cybercriminals, to respond to requests for assistance, if possible in real time, to secure the supply chain of companies in their countries, to report on potential vulnerabilities to third parties to assist them in preventing future incidents, and in particular to support and protect all cyber incident response teams within and beyond their borders; **220**

(Pakistan)

Amend to read as follows:

8. ~~*Encourages*~~ ***Urges*** parliaments to promote a secure cyberspace by calling on their governments to cooperate in stopping cybercrime and cybercriminals, to respond to requests for assistance, if possible in real time, to secure the supply chain ~~of companies in their countries~~ **with service providers in each country**, to report on potential vulnerabilities to third parties to assist them in preventing future incidents, and in particular to support and protect all cyber incident response teams within and beyond their borders; **221**

(Nicaragua)

Amend to read as follows:

8. *Encourages* parliaments to promote ~~a~~ **an open, free and** secure cyberspace by calling on their governments to cooperate in ~~stopping~~ **fighting** cybercrime and cybercriminals, to respond to requests for assistance, if possible in real time, to secure the supply chain of companies in their countries, to report on potential vulnerabilities to third parties to assist them in preventing future incidents, and in particular to support and protect all cyber incident response teams within and beyond their borders; **222**

(Czech Republic)

Amend to read as follows:

8. *Encourages* parliaments to promote a secure cyberspace by calling on their governments to **abide by the United Nations norms of responsible State behaviour in cyberspace and** cooperate in stopping cybercrime and cybercriminals, to respond to requests for assistance, if possible in real time, to secure the supply chain of companies in their countries, to report on potential vulnerabilities to third parties to assist them in preventing future incidents, and in particular to support and protect all cyber incident response teams within and beyond their borders; **223**

(Canada)

Amend to read as follows:

8. *Encourages* parliaments to promote a secure cyberspace by calling on their governments to cooperate in ~~stopping~~ **preventing and fighting** cybercrime ~~and cybercriminals~~, to respond to requests for assistance, if possible in real time, to secure the supply chain of companies in their countries, to report on potential vulnerabilities to third parties to assist them in preventing future incidents, and in particular to support and protect all cyber incident response teams within and beyond their borders; **224**

(Lithuania)

Amend to read as follows:

8. *Encourages* parliaments to promote a secure cyberspace by calling on their governments to cooperate in ~~stopping~~ **mitigating the consequences of** ~~cybercrime~~ **cyberattacks** and ~~cybercriminals~~ **cybercrime**, to respond to requests for assistance, if possible in real time, to secure the supply chain of companies in their countries, to report on potential vulnerabilities to third parties to assist them in preventing future incidents, and in particular to support and protect all cyber incident response teams within and beyond their borders; **225**

(Argentina)

Amend to read as follows:

8. *Encourages* parliaments to promote a secure cyberspace by calling on their governments to cooperate in stopping cybercrime and cybercriminals, to respond to requests for assistance **and exchange of information on cyber incidents and cybercriminals**, if possible in real time, to secure the supply chain of companies in their countries, to report on potential vulnerabilities to third parties to assist them in preventing future incidents, and in particular to support and protect all cyber incident response teams within and beyond their borders; **226**

(Ukraine)

Amend to read as follows:

8. *Encourages* parliaments to promote a secure cyberspace by calling on their governments to cooperate in stopping cybercrime and cybercriminals, to respond to requests for assistance, if possible in real time, **in accordance with the rule of law and fully respecting international human rights law and fundamental freedoms**, to secure the supply chain of companies in their countries, to report on potential vulnerabilities to third parties to assist them in preventing future incidents, and in particular to support and protect all cyber incident response teams within and beyond their borders; **227**

(Germany)

Amend to read as follows:

8. *Encourages* parliaments to promote a secure cyberspace by calling on their governments to cooperate in stopping cybercrime and cybercriminals, to respond to requests for assistance, if possible in real time, to secure the supply chain of companies in their countries, to report on potential vulnerabilities ~~to third parties to~~ **and** assist ~~them~~ in preventing future incidents, and in particular to support and protect all cyber incident response teams within and beyond their borders; **228**

(India)

Operative paragraph 9

Amend to read as follows:

9. *Also encourages* parliaments to draft legislation promoting cross-cutting cybersecurity services that prioritize prevention (awareness-raising, auditing and training), incident detection (24 hours a day, 7 days a week), and an instant and efficient response to ~~cyber~~ **ICT** threats; **229**

(Islamic Republic of Iran)

Amend to read as follows:

9. *Also encourages* parliaments to draft legislation promoting cross-cutting cybersecurity services that prioritize prevention (awareness-raising, auditing and training), incident detection (24 hours a day, 7 days a week), and an instant and efficient response to cyber threats**, where they do not yet exist in their country**; **230**

(Nicaragua)

Amend to read as follows:

9. *Also encourages* parliaments to draft legislation promoting cross-cutting ~~cybersecurity~~ services **for security in the use of information and communications technologies, hereinafter referred to as "cybersecurity",** that prioritize prevention (awareness-raising, auditing and training), incident detection (24 hours a day, 7 days a week), and an instant and efficient response to **threats to security in the use of information and communications technologies, hereinafter referred to as "**cyber threats**"**; **231**

(Russian Federation)

Operative paragraph 10

Amend to read as follows:

10. *Recommends* that parliaments ~~establish~~ **promote the establishment of** relevant institutions and bodies – such as national cybersecurity centres, computer emergency response teams, computer security incident response teams and security operations centres – where these do not already exist in their country; **232**

(Romania)

Amend to read as follows:

10. *Recommends* that parliaments **advise their respective governments to** establish relevant institutions and bodies **for cybercrime and cyberattack prevention** – such as national cybersecurity centres, computer emergency response teams, computer security incident response teams and security operations centres – where these do not already exist in their country; **233**

(Thailand)

Operative paragraph 11

Amend to read as follows:

11. *Also recommends* that ~~all~~ parliaments ensure that such institutions and bodies have adequate budgetary resources and specialized personnel to allow for an agile and effective response to cyberattacks and to protect critical infrastructure, public institutions, companies and citizens; **234**

(Republic of Korea)

Amend to read as follows:

11. *Also recommends* that all parliaments ensure that such institutions and bodies have adequate budgetary resources and specialized personnel, **trained in human rights principles and practices,** to allow for an agile and effective response to cyberattacks and to protect critical infrastructure, public institutions, companies and citizens; **235**

(Canada)

Amend to read as follows:

11. *Also recommends* that all parliaments ensure that such institutions and bodies have adequate budgetary resources and specialized personnel to allow for **the prevention and detection of, and** an agile and effective response to**,** cyberattacks**,** ~~and to protect~~ **particularly the protection of vulnerable and** critical infrastructure **(such as air traffic management systems and electrical power grids)**, public institutions **(such as hospitals and health services)**, companies and citizens; **236**

(Philippines)

Amend to read as follows:

11. *Also recommends* that all parliaments ensure that such institutions and bodies have adequate budgetary resources and specialized personnel to allow for an agile and effective response to **cybercrime and** cyberattacks and to protect critical infrastructure, public institutions, companies and citizens; **237**

(Belgium)

Amend to read as follows:

11. *Also recommends* that all parliaments ensure that such institutions and bodies have adequate budgetary resources and specialized personnel to allow for an agile and effective response to ~~cyberattacks~~ **ICT threats** and to protect critical infrastructure, public institutions, companies and citizens; **238**

(Islamic Republic of Iran)

Amend to read as follows:

11. *Also recommends* that all parliaments ensure that such institutions and bodies have adequate budgetary resources and specialized personnel to allow for an agile**, timely** and effective response to cyberattacks and to protect critical infrastructure, public institutions, companies and citizens **without breaching privacy**; **239**

(Thailand)

Amend to read as follows:

11. *Also recommends* that all parliaments ensure that such institutions and bodies have adequate budgetary resources and specialized personnel to allow for an agile and effective response to cyberattacks and to protect critical **civilian** infrastructure, public institutions, companies and citizens; **240**

(Sweden)

Amend to read as follows:

11. *Also recommends* that all parliaments ensure that such institutions and bodies have adequate budgetary resources and specialized personnel to allow for an agile and effective response to cyberattacks and to protect critical infrastructure, public institutions, companies and citizens**, taking into account that the increasing digitalization of public services and utilities could imply major exposure to digital risks**; **241**

(Argentina)

New operative paragraph 11bis

11bis. *Invites* parliaments to encourage their governments to provide specific cybersecurity training in order to help increase the number of cybersecurity professionals and to strengthen their performance; **242**

(Thailand)

Operative paragraph 12

Delete the paragraph. **243**

(Belgium, Canada, Egypt, Japan, Russian Federation)

Amend to read as follows:

12. *Urges* parliaments to promote international coordination between such institutions and bodies ~~and the creation of a global security operations centre, under the auspices of the United Nations,~~ in order to ~~constantly~~ monitor, prevent, detect, investigate and respond to cyber threats; **244**

(Switzerland)

Amend to read as follows:

12. *Urges* parliaments to promote international coordination between such institutions and bodies ~~and the creation of a global security operations centre, under the auspices of the United Nations,~~ in order to constantly monitor, prevent, detect, investigate and respond to cyber threats; **245**

(Germany)

Amend to read as follows:

12. *Urges* parliaments to promote international coordination between such institutions and bodies and the creation of a global ~~security operations~~ **cybersecurity** centre, under the auspices of the United Nations, in order to constantly monitor, prevent, detect, investigate and respond to cyber threats; **246**

(France)

Amend to read as follows:

12. *Urges* parliaments to promote international coordination between such institutions and bodies and the creation of a global security operations centre, under the auspices of the United Nations, in order to constantly monitor, ~~prevent,~~ detect, investigate, and respond to **global** cyber threats **in cooperation with the national cyber incident response teams of Member States so as to support the prevention of these threats**; **247**

(Türkiye)

Amend to read as follows:

12. *Urges* parliaments to promote international coordination between such institutions and bodies and the creation of a global security operations centre, under the auspices of the United Nations, in order to constantly monitor, prevent, detect, investigate and respond to ~~cyber~~ **ICT** threats; **248**

(Islamic Republic of Iran)

Amend to read as follows:

12. *Urges* parliaments to promote international coordination between such institutions and bodies and the creation of a global security operations centre, under the auspices of the United Nations, in order to constantly monitor, prevent, detect, investigate and respond to cyber threats**, while clearly defining the scope of its mandate in relation to other relevant United Nations bodies, such as the United Nations Chief Executives Board, through the High-Level Committee on Programmes and the United Nations-wide framework on cybersecurity and cybercrime**; **249**

(Sweden)

New operative paragraph 12bis

12bis. *Calls on* governments and the international community to collaborate on ways to expose the actors and entities behind these cyberattacks and to make them accountable for their actions through the filing of criminal cases and the imposition of applicable sanctions; **250**

(Philippines)

Operative paragraph 13

Delete the paragraph. **251**

(Belgium, Canada, Egypt, Germany, Russian Federation, Switzerland)

Amend to read as follows:

13. *Recommends* that ~~such an entity support~~ **technical assistance and capacity-building be provided to** all States, and especially those with fewer resources, in developing action and response capabilities, in sharing intelligence, knowledge and research in anticipation of future ~~technology-related challenges such as quantum computing, 5G, the metaverse or Artificial Intelligence~~ **technologies**, and in ~~raising the alarm should~~ **alerting if, in any circumstances,** the Universal Declaration of Human Rights **were to** be violated ~~in any circumstances~~; **252**

(Czech Republic)

Amend to read as follows:

13. *Recommends* that such an entity support ~~all~~ States, and especially those with fewer resources, in developing action and response capabilities, in sharing intelligence, knowledge and research in anticipation of future technology-related challenges such as quantum computing, 5G, the metaverse and artificial intelligence, and in raising the alarm should the Universal Declaration of Human Rights be violated in any circumstances; **253**

(Republic of Korea)

Amend to read as follows:

13. *Recommends* that such an entity support all States, and especially ~~those with fewer resources~~ **developing ones**, in developing action and response capabilities, in sharing intelligence, knowledge and research in anticipation of future technology-related challenges such as quantum computing, 5G, the metaverse and artificial intelligence, and in raising the alarm should the Universal Declaration of Human Rights be violated in any circumstances; **254**

(Islamic Republic of Iran)

Amend to read as follows:

13. *Recommends* that such an entity support all States, and especially those with fewer resources, in developing action and response capabilities, **and** in sharing intelligence, knowledge and research in anticipation of future technology-related challenges such as quantum computing, 5G, the metaverse and artificial intelligence~~, and in raising the alarm should the Universal Declaration of Human Rights be violated in any circumstances~~; **255**

(India)

Amend to read as follows:

13. *Recommends* that such an entity support all States, and especially those with fewer resources, in developing action and response capabilities, in sharing intelligence, knowledge and research in anticipation of future technology-related challenges such as quantum computing, 5G, the metaverse and artificial intelligence, and in~~ raising the alarm should the Universal Declaration of Human Rights be violated in any circumstances~~ **increasing their resilience to cyber threats**; **256**

(France)

Amend to read as follows:

13. *Recommends* that such an entity support all States, and especially those with fewer resources, in developing action and response capabilities, in sharing intelligence, knowledge and research in anticipation of future technology-related challenges such as quantum computing, 5G, the metaverse and artificial intelligence, and in raising the alarm should ~~the Universal Declaration of Human Rights be violated in any circumstances~~ **violations of universally recognized human rights be caused by developments in its area of responsibility**; **257**

(Ukraine)

Amend to read as follows:

13. *Recommends* that such an entity support all States, and especially those with fewer resources, in developing action and response capabilities, in sharing intelligence, knowledge and research in anticipation of future technology-related challenges such as quantum computing, 5G, the metaverse and artificial intelligence, and in raising the alarm should the Universal Declaration of Human Rights **or other human rights instruments** be violated in any circumstances; **258**

(Sweden)

New operative paragraph 13bis

13bis. *Reaffirms* that an open, secure, stable, accessible and peaceful ICT environment is essential for all and requires effective cooperation among States to reduce risks to international peace and security, and *calls upon* the international community to promote full respect for human rights and fundamental freedoms; **259**

(Germany)

Operative paragraph 14

Delete the paragraph. **260**

(India)

Amend to read as follows:

14. *Calls upon* parliaments to encourage investment in research and development, incorporating into the design of each project specific ~~cybersecurity~~ **ICT security** provisions, with appropriate budget allocation, in order to anticipate and protect against possible emerging ~~cyber~~ **ICT** threats; **261**

(Islamic Republic of Iran)

Operative paragraph 15

Delete the paragraph. **262**

(India)

Amend to read as follows:

15. *Encourages* parliaments to partner with industry, academia and all other stakeholders, including civil society, in order to foster a strong and collaborative ~~cybersecurity~~ **ICT security** ecosystem; **263**

(Islamic Republic of Iran)

Amend to read as follows:

15. *Encourages* parliaments to partner with industry, academia and all other stakeholders, including civil society, **with their respective governments as key facilitators,** in order to foster a strong and collaborative cybersecurity ecosystem; **264**

(Thailand)

Amend to read as follows:

15. *Encourages* parliaments to partner with industry, academia and all other stakeholders, including civil society, in order to foster a strong and collaborative cybersecurity ecosystem **that fully respects human rights principles and international human rights obligations**; **265**

(Canada)

Amend to read as follows:

15. *Encourages* parliaments to partner with industry, academia and all other stakeholders, including civil society, in order to foster a strong and collaborative cybersecurity ecosystem**, without prejudice to the establishment of regimes that guarantee that internet service and application providers deliver information promptly on the traces and indications that the judicial courts of different countries request, to the extent that such information may constitute digital evidence for the investigation of cybercrime at the local level, regardless of their regional headquarters or the privacy regulations of the country in which such information is stored**; **266**

(Argentina)

Operative paragraph 16

Delete the paragraph. **267**

(Belgium, Canada)

Amend to read as follows:

16. *Also encourages* parliaments to develop ~~legislative spaces where~~ **trust, such that** parliaments, governments, companies, academia and civil society can cooperate in real time in order to defend the general interests of all States; **268**

(India)

Amend to read as follows:

16. *Also encourages* parliaments to develop legislative spaces where parliaments, governments, companies, academia and civil society can cooperate in real time**, in accordance with rule of law and fully respecting international human rights law and fundamental freedoms,** in order to defend the general interests of all States; **269**

(Germany)

New operative paragraph 16bis

16bis. *Calls upon* parliaments and their governments to address the lack of responsibility of service providers and transnational platforms, which poses a serious threat in the ICT environment; **270**

(Islamic Republic of Iran)

Operative paragraph 17

Amend to read as follows:

17. *Calls upon* parliaments and parliamentarians to actively engage in promoting a shared, up-to-date national understanding of the nature of ~~cybercrime~~ **the use of information and communications technologies for criminal purposes** and ~~cyberattacks~~ **ICT threats** as experienced by citizens, organizations and institutions; **271**

(Islamic Republic of Iran)

Amend to read as follows:

17. *Calls upon* parliaments and parliamentarians to actively engage in promoting a shared, up-to-date national understanding of the nature of ~~cybercrime~~ **misuse of ICT for criminal purposes** and cyberattacks as experienced by citizens, organizations and institutions; **272**

(Pakistan)

Amend to read as follows:

17. *Calls upon* parliaments and parliamentarians to actively engage in promoting a shared, up-to-date national understanding of the nature of cybercrime ~~and cyberattacks~~ as experienced by citizens, organizations and institutions; **273**

(Belgium, Czech-Republic, Sweden)

Amend to read as follows:

17. *Calls upon* parliaments and parliamentarians to actively engage in promoting a shared, up-to-date national understanding of the nature of cybercrime and cyberattacks as experienced by citizens, organizations and institutions**, where they do not yet exist in their country**; **274**

(Nicaragua)

Operative paragraph 18

Delete the paragraph. **275**

(India)

Amend to read as follows:

18. *Urges* parliaments to help foster a true “culture of cybersecurity” by developing educational curricula focused on training future generations, from childhood onwards, in ~~the correct use of~~ **digital literacy and** technological ~~devices~~ **know-how**, covering both the great opportunities they present and the serious risks they pose; **276**

(Thailand)

New operative paragraph 18bis

18bis. *Also urges* parliaments, in all their activities related to combating cybercrime and malicious cyber incidents, to promote obligations under international human rights law and full respect for human rights and fundamental freedoms and the rule of law; **277**

(Canada)

Operative paragraph 19

Delete the paragraph. **278**

(Islamic Republic of Iran)

Amend to read as follows:

19. *Recommends* that parliaments broaden protections for ~~women, young people and other~~ vulnerable groups, **especially children and the elderly,** in cyberspace, taking respect for human rights and the prevention of gender-based violence into account in the development of educational policies on the use of social media; **279**

(Germany)

Amend to read as follows:

19. *Recommends* that parliaments broaden protections for women, ~~young people~~ **children, the elderly** and other vulnerable groups in cyberspace, taking **into account** respect for human rights and the prevention of gender-based violence ~~into account~~ in the development of educational policies on the use of social media; **280**

(Czech Republic)

Amend to read as follows:

19. *Recommends* that parliaments broaden protections for women, young **and elderly** people, **children** and other vulnerable groups in cyberspace, taking respect for human rights and the prevention of gender-based violence into account in the development of educational policies on the use of social media; **281**

(Viet Nam)

Amend to read as follows:

19. *Recommends* that parliaments broaden protections for women, **children,** young people and other vulnerable groups in cyberspace, taking respect for human rights and the prevention of gender-based violence into account in the development of educational policies on the use of social media; **282**

(Romania)

Amend to read as follows:

19. *Recommends* that parliaments broaden protections for women, young people**, the elderly** and other vulnerable groups in cyberspace, taking respect for human rights and the prevention of gender-based violence into account in the development of educational policies on the use of social media; **283**

(Türkiye)

Amend to read as follows:

19. *Recommends* that parliaments broaden protections for women, young people**, racialized communities** and other vulnerable groups in cyberspace, taking respect for human rights and the prevention of gender-based violence into account in the development of educational policies on the use of social media; **284**

(Canada)

Amend to read as follows:

19. *Recommends* that parliaments broaden protections for women, young people**, persons with disabilities** and other vulnerable groups in cyberspace, taking respect for human rights and the prevention of gender-based violence into account in the development of educational policies on the use of social media; **285**

(Finland)

New operative paragraph 19bis

19bis. *Calls on* parliaments to convene a multi-stakeholder collaboration between government and the private sector in order to institutionalize technology as a tool to raise awareness about sexual harassment and to combat cyber violence against women and children; **286**

(Philippines)

Operative paragraph 20

Delete the paragraph. **287**

(India)

Amend to read as follows:

20. *Urges* parliaments to take the necessary action to ~~protect critical moments in democracy, and especially those periods when citizens exercise their right to vote, in order to avoid attacks and interferences that seek to influence, change or violate the free formation of public opinion during the electoral process~~ **prevent interference in a State's internal affairs through the use of information and communications technologies**; **288**

(Russian Federation)

Operative paragraph 21

Delete the paragraph. **289**

(India, Islamic Republic of Iran)

Amend to read as follows:

21. *Calls upon* the international community to take action to protect ~~democracy~~ **the information and communications technology systems of government authorities** by ensuring that all parliaments worldwide, as institutions representing the will of the people, are afforded special protection through their inclusion in lists of critical national infrastructure and essential services; **290**

(Russian Federation)

Amend to read as follows:

21. *Calls upon* the international community to take action to protect democracy by ensuring that all parliaments worldwide, as institutions representing the will of the people, are afforded special protection through their inclusion in lists of critical ~~national~~ **civilian** infrastructure and essential services; **291**

(Sweden)

New operative paragraph 21bis

21bis. *Stresses* the need to further enhance international cooperation and assistance in the area of ICT security and capacity-building, as a means to bridge digital divides and strengthen the response to cyber threats globally; **292**

(Romania)

Operative paragraph 22

Amend to read as follows:

22. *Calls upon* parliaments to deepen their understanding of the complex and rapid nature of ~~cybercrime~~ **the use of information and communications technologies for criminal purposes** and ~~cyberattacks~~ **ICT threats** by holding specialized seminars, workshops and conferences on this subject; **293**

(Islamic Republic of Iran)

Amend to read as follows:

22. *Calls upon* parliaments to deepen their understanding of the complex and rapid nature of cybercrime and ~~cyberattacks~~ **cyber incidents** by holding specialized seminars, workshops and conferences on this subject; **294**

(India)

Amend to read as follows:

22. *Calls upon* parliaments to deepen their understanding of the complex and rapid nature of ~~cybercrime~~ **misuse of ICT for criminal purposes** and cyberattacks by holding specialized seminars, workshops and conferences on this subject; **295**

(Pakistan)

Amend to read as follows:

22. *Calls upon* parliaments to deepen their understanding of the complex and ~~rapid~~ **rapidly evolving** nature of cybercrime ~~and cyberattacks~~ by holding specialized seminars, workshops and conferences on this subject; **296**

(Sweden)

Amend to read as follows:

22. Calls upon parliaments to deepen their understanding of the complex and rapid nature of cybercrime and cyberattacks by **enabling the open sharing of knowledge, experience and expertise by** holding specialized seminars, workshops and conferences on this subject; **297**

(South Africa)

Amend to read as follows:

22. *Calls upon* parliaments to deepen their understanding of the complex and rapid nature of cybercrime and cyberattacks by holding specialized seminars, workshops and conferences on this subject**, where they do not yet exist in their country**; **298**

(Nicaragua)

Operative paragraph 23

Delete the paragraph. **299**

(Russian Federation)

Amend to read as follows:

23. *Invites* the IPU ~~Secretariat~~, in partnership with other relevant organizations, to promote this new vision of cybersecurity by supporting parliaments in their capacity-building endeavours; **300**

(Belgium)

Amend to read as follows:

23. *Invites* the IPU Secretariat, in partnership with other relevant organizations, to promote this new vision of ~~cybersecurity~~ **ICT security** by supporting parliaments in their capacity-building endeavours; **301**

(Islamic Republic of Iran)

Amend to read as follows:

23. *Invites* the IPU Secretariat, in partnership with other relevant organizations, to promote this new vision of cybersecurity by supporting parliaments in their capacity-building endeavours**, and to set its strategic goal in encouraging parliaments to create in-house cybersecurity intelligence centres for sharing and exchanging their information, intelligence, expertise and best practices, with a view to expanding common knowledge of cybersecurity**; **302**

(Thailand)

Operative paragraph 24

Amend to read as follows:

24. *Recommends* that the IPU~~, as the global organization of parliaments, play a leading role in international internet governance and cyber resilience by participating in all relevant international forums, including those led by the United Nations, with a view to ensuring that the voice of parliaments is heard, in order to anticipate, prepare for, resist, respond to and recover from any cyber threat to the security, livelihood or way of life of the people~~ **contribute to the internationalization of internet management, to the equal participation of all States in this process, and to the preservation of the sovereign right of States to regulate the national segment of the global internet network**. **303**

(Russian Federation)

Amend to read as follows:

24. *Recommends* that the IPU, as the global organization of parliaments, play a leading role in ~~international internet governance~~ **preventing and combating cybercrime** and **stimulating** cyber-resilience by participating in all relevant international forums, including those led by the United Nations, with a view to ensuring that the voice of parliaments is heard, in order to anticipate, prepare for, resist, respond to and recover from any cyber threat to the security, livelihood, **human rights** or way of life of the people. **304**

(Belgium)

Amend to read as follows:

24. *Recommends* that the IPU, as the global organization of parliaments, play a leading role in international internet governance and cyber resilience by ~~participating in all~~ **strengthening partnerships with** relevant international forums, including those led by the United Nations, with a view to ensuring that the voice of parliaments is heard, in order to anticipate, prepare for, resist, respond to and recover from any cyber threat to the security, livelihood or way of life of the people. **305**

(Republic of Korea)

Amend to read as follows:

24. *Recommends* that the IPU, as the global organization of parliaments, play a leading role in international internet governance and cyber resilience by participating in all relevant international forums, including those led by the United Nations, with a view to ensuring that the voice of parliaments is heard~~, in order to anticipate, prepare for, resist, respond to and recover from any cyber threat to the security, livelihood or way of life of the people~~. **306**

(France)

Amend to read as follows:

24. *Recommends* that the IPU, as the global organization of parliaments, play a leading role in international internet governance and cyber resilience by participating in all relevant international forums, including those led by the United Nations, with a view to ensuring that the voice of parliaments is heard, in order to anticipate, prepare for, resist, respond to and recover from any ~~cyber~~ **ICT** threat to the security, livelihood or way of life of the people. **307**

(Islamic Republic of Iran)

Amend to read as follows:

24. *Recommends* that the IPU, as the global organization of parliaments, play a leading role in international internet governance and cyber resilience by participating in all relevant international forums, including those led by the United Nations, with a view to ensuring that the voice of parliaments is heard, in order to anticipate, prepare for, resist, respond to and recover from any cyber threat to the security, livelihood or way of life of the people**, after consultation with the States Parties**. **308**

(Nicaragua)

New operative paragraph 24bis

24bis. *Promotes* the creation of a working group on cyberattacks and cybercrime, under the Governing Council of the IPU, whose specific mission shall be to comply with the mandates and objectives established in this resolution, and whose powers shall include both supporting the process for the promotion of an international convention on cybercrime within the framework of the United Nations, and strengthening the capacities of IPU national Member Parliaments in terms of law-making, oversight and budgeting; **309**

(Argentina)

24bis. ***Also recommends*** **that the IPU raise awareness among parliaments on achieving the SDGs through, above all else, their universal commitments to digital security.** **310**

(Thailand)

New operative paragraph 24ter

24ter. ***Urges*** **international organizations to discuss a convention on acts of cyberwar within the framework of maintaining international peace and security**. **311**

(Argentina)

TITLE

Modify the title as follows:

~~Cyberattacks and~~ ~~cybercrimes~~ **Cybercrimes**: The new risks to global security **312**

(Czech Republic)

Modify the title as follows:

~~Cyberattacks and~~ ~~cybercrimes~~ **Cyber incidents and cyber crimes**: The new risks to global security **313**

(India)

Modify the title as follows:

~~Cyberattacks and~~ ~~cybercrimes~~ **ICT threat and the use of information and communications technologies for criminal purposes**: The new risks to global security **314**

(Islamic Republic of Iran)

Modify the title as follows:

Cyberattacks and cybercrimes: The ~~new~~ **increased** risks to global security **315**

(Lithuania)

Modify the title as follows:

Cyberattacks and ~~cybercrimes~~ **misuse of ICT for criminal purposes**: The new risks to global security **316**

(Pakistan)

Modify the title as follows:

~~Cyberattacks and cybercrimes~~ **Cybercrimes**: The ~~new~~ **evolving** risks to global security **317**

(Sweden)