United Nations A/RES/78/237

General Assembly

Distr.: General
28 December 2023

Seventy-eighth session
Agenda item 94
Developments in the field of information and telecommunications in the context of international security

Resolution adopted by the General Assembly on 22 December 2023

[*on the report of the First Committee (A/78/404, para. 14)*]

78/237. Developments in the field of information and telecommunications in the context of international security

The General Assembly,

Recalling its resolutions 36/103 of 9 December 1981, 43/78 H of 7 December 1988, 53/70 of 4 December 1998, 54/49 of 1 December 1999, 55/28 of 20 November 2000, 56/19 of 29 November 2001, 57/53 of 22 November 2002, 58/32 of 8 December 2003, 59/61 of 3 December 2004, 60/45 of 8 December 2005, 61/54 of 6 December 2006, 62/17 of 5 December 2007, 63/37 of 2 December 2008, 64/25 of 2 December 2009, 65/41 of 8 December 2010, 66/24 of 2 December 2011, 67/27 of 3 December 2012, 68/243 of 27 December 2013, 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, 76/19 of 6 December 2021 and 77/36 of 7 December 2022,

Commemorating the twenty-fifth anniversary of discussions, under the auspices of the United Nations, on developments in the field of information and telecommunications in the context of international security,

Stressing that it is in the interest of all States to promote the use of information and communications technologies for peaceful purposes, with the objective of shaping a community of shared future for humankind for peace, security and stability in the information space, and that States also have an interest in the prevention and peaceful settlement of conflicts arising from the use of such technologies,

Confirming that information and communications technologies are dual-use technologies and can be used for both legitimate and malicious purposes,

Expressing concern that these technologies and means can potentially be used for purposes that are inconsistent with the objectives of maintaining international peace and security and may adversely affect the integrity of the infrastructure of States, to the detriment of their security in both civil and military fields,

Recalling that a number of States are developing information and communications technology capabilities for military purposes and that the use of information and communications technologies in future conflicts between States is becoming more likely,

Reaffirming that, in accordance with Article 2 (4) of the Charter of the United Nations, all States Members of the United Nations shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the purposes of the United Nations,

Recognizing that the indication that an information and communications technology activity was launched or otherwise originates from the territory or objects of the information and communications technology infrastructure of a State may be insufficient in itself to attribute the activity to that State, and noting that accusations of organizing and implementing wrongful acts brought against States should be substantiated,

Considering the growth and aggregation of data associated with new and emerging technologies, and noting the increasing relevance of data protection and data security and the need to continue to study, with a view to promoting common understandings, existing and potential threats in the sphere of information security, inter alia, data security, and possible cooperative measures to prevent and counter such threats,

Expressing concern about the possibility of embedding harmful hidden functions in information and communications technologies that can be used to undermine the secure and reliable use of such technologies and the information and communications technology supply chain for products and services, erode trust in commerce and damage national security, and reaffirming that reasonable steps to promote openness and ensure the integrity, stability and security of the supply chain can include putting in place at the national level comprehensive, transparent, objective and impartial frameworks and mechanisms for supply chain risk management consistent with a State’s international obligations, increased attention in national policy and in dialogue with States and relevant actors at the United Nations and other forums on how to ensure that all States can compete and innovate on an equal footing, and developing and implementing global common rules and standards for supply chain security, and stressing in this regard the necessity of compliance by producers and suppliers of information and communications technology goods and services with the legislation of States on whose territories they operate,

Reaffirming that, in accordance with the principle of non-intervention, States must not intervene directly or indirectly in the internal affairs of another State, including by means of information and communications technologies,

Recognizing the duty of a State to abstain from any defamatory campaign, vilification or hostile propaganda for the purpose of intervening or interfering in the internal affairs of other States,

Recognizing also that the dissemination and use of information and communications technologies affect the interests of the entire global community and that broad international cooperation leads to the most effective universal responses to address information and communications technology threats and promotes an open, secure, stable, accessible and peaceful information and communications technology environment, *Reaffirming* that the United Nations should continue to play a leading role in promoting dialogue on the use of information and communications technologies by States,

Underlining the importance for the global community of shaping a system of international information security and continuing a democratic, inclusive, transparent and results-oriented negotiation process within the Open-ended Working Group on security of and in the use of information and communications technologies 2021–2025, while recognizing its centrality as the mechanism within the United Nations for dialogue on security in the use of information and communications technologies,

Reaffirming that, given the unique attributes of information and communications technologies, additional norms could be developed over time, and noting the need to further consider the development of additional legally binding obligations, taking into account in this regard specific proposals of States on establishing an international legal regime to regulate the information and communications technology field,

Noting that capacity-building is essential for international security, cooperation of States and confidence-building in the field of information and communications technology security and that capacity-building measures should seek to promote the use of information and communications technologies for peaceful purposes, and that further focused discussions and decisions within the Open-ended Working Group are needed on funding specifically for capacity-building efforts on security in the use of information and communications technologies, in particular for information and communications technology development of requesting States,

Welcoming the efforts of the Chair of the Open-ended Working Group to forge consensus among States on the common goal of ensuring an open, stable, secure, accessible and peaceful information and communications technology environment,

1. *Supports* the work of the Open-ended Working Group on security of and in the use of information and communications technologies 2021–2025 in accordance with its mandate, as enshrined in General Assembly resolution 75/240;

2. *Calls upon* States to further engage constructively in the negotiations during formal and intersessional meetings of the Open-ended Working Group, which, pursuant to its mandate, will present recommendations, adopted by consensus, to the General Assembly;

3. *Welcomes* the adoption by consensus of the second annual progress report of the Open-ended Working Group,[1] and takes note of the compendium of statements in explanation of position on its adoption;[2]

4. *Also welcomes* the establishment of the global intergovernmental points of contact directory as the first universal confidence-building measure, and calls upon States to use this instrument in good faith to develop practical cooperation, including through the computer emergency response teams channels, as well as to continue discussing at the Open-ended Working Group possible ways to continuously improve the directory in an incremental and step-by-step manner, as set out in annex A to the second annual progress report of the Open-ended Working Group, inter alia, through communication protocols and required capacity-building measures;

5. *Recommends* that Member States continue discussions at the Open-ended Working Group, in accordance with its mandate, on rules, norms and principles of

[1] See A/78/265.

[2] A/AC.292/2023/INF/5.

responsible behaviour of States, including the need to discuss the elaboration of additional legally binding obligations;

6. *Encourages* Member States to continue exchanging views at the Open-ended Working Group on intergovernmental regular institutional dialogue on security in the use of information and communications technologies, with the objective of elaborating a common understanding on the most effective format for future regular institutional dialogue with the broad participation of States under United Nations auspices to be established upon conclusion of the work of the Open-ended Working Group, and confirms that, in considering different proposals on regular institutional dialogue, the views, concerns and interests of all States should be taken into account, and recommends that these proposals be further elaborated within the Open-ended Working Group;

7. *Invites* Member States to share within the Open-ended Working Group their views on capacity-building needs, including for the implementation of practical measures recommended by the Open-ended Working Group, as well as possible inclusive mechanisms to meet them, including funding, taking into account the agreed principles of capacity-building, as set out in annex C to the second annual progress report of the Open-ended Working Group, in particular that capacity-building activities should correspond to nationally identified needs and priorities and should be undertaken with full respect for the principle of State sovereignty;

8. *Invites* all Member States to continue to inform the Secretary-General of their views and assessments on security of and in the use of information and communications technologies, in particular on the future regular institutional dialogue on these matters under the auspices of the United Nations, and requests the Secretary-General to submit a report based on those views to the General Assembly during its seventy-eighth session for further discussion between Member States in the meetings of the Open-ended Working Group at its eighth session in 2024;

9. *Decides* to include in the provisional agenda of its seventy-ninth session the item entitled "Developments in the field of information and telecommunications in the context of international security".

50th (resumed) plenary meeting
22 December 2023