United Nations A/C.1/73/L.27*

General Assembly

Distr.: Limited
22 October 2018

Original: English

Seventy-third session
First Committee
Agenda item 96
Developments in the field of information and telecommunications in the context of international security

Algeria, Angola, Azerbaijan, Belarus, Bolivia (Plurinational State of), Burundi, Cambodia, China, Cuba, Democratic People's Republic of Korea, Democratic Republic of the Congo, Eritrea, Kazakhstan, Madagascar, Namibia, Nepal, Nicaragua, Pakistan, Russian Federation, Samoa, Sierra Leone, Suriname, Syrian Arab Republic, Tajikistan, Uzbekistan, Venezuela (Bolivarian Republic of) and Zimbabwe: draft resolution

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 and 71/28 of 5 December 2016,

Noting that considerable progress has been achieved in developing and applying the latest information technologies and means of telecommunication,

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

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

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 in cyberspace, and that States also have an interest in preventing conflict arising from the use of information and communications technologies,

* Reissued for technical reasons on 24 October 2018.

Noting that the United Nations should play a leading role in promoting dialogue among Member States to develop common understandings on the security of and the use of information and communications technologies, as well as in developing common understandings on the application of international law and norms, rules and principles for responsible State behaviour in this sphere, encourage regional efforts, promote confidence-building and transparency measures and support capacity-building and the dissemination of best practices,

Expressing concern that embedding harmful hidden functions in information and communications technologies could be used in ways that would affect 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,

Considering that it is necessary to prevent the use of information resources or technologies for criminal or terrorist purposes,

Underlining the need for enhanced coordination and cooperation among States in combating the criminal misuse of information technologies, and in that context stressing the role that can be played by the United Nations and other international and regional organizations,

Underlining also the importance of respect for human rights and fundamental freedoms in the use of information and communications technologies,

Welcoming the effective work of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security and the relevant outcome reports transmitted by the Secretary-General,[1]

Welcoming also that, in considering the application of international law to State use of information and communications technologies, the Group of Governmental Experts, in its 2015 report,[2] identified as of central importance the commitments of States to the following principles of the Charter of the United Nations and other international law: sovereign equality; the settlement of international disputes by peaceful means in such a manner that international peace and security and justice are not endangered; refraining 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; respect for human rights and fundamental freedoms; and non-intervention in the internal affairs of other States,

Confirming the conclusions of the Group of Governmental Experts, in its 2013[3] and 2015[2] reports, that international law, and in particular the Charter, is applicable and essential to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful information and communications technology environment, that voluntary and non-binding norms, rules and principles of responsible behaviour of States in the use of information and communications technologies can reduce risks to international peace, security and stability, and that, given the unique attributes of such technologies, additional norms can be developed over time,

Confirming also that State sovereignty and international norms and principles that flow from sovereignty apply to the conduct by States of information and

[1] A/65/201, A/68/98 and A/70/174.
[2] A/70/174.
[3] A/68/98.

communications technology-related activities and to their jurisdiction over information and communications technology infrastructure within their territory,

Noting that capacity-building is essential for cooperation of States and confidence-building in the field of information and communications technology security,

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 cybersecurity best practices and training, pursuant to General Assembly resolution 64/211 of 21 December 2009, entitled "Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures",

Stressing also that, while States have a primary responsibility for maintaining a secure and peaceful information and communications technology environment, effective international cooperation would benefit from identifying mechanisms for the participation, as appropriate, of the private sector, academia and civil society organizations,

1. *Welcomes* the following set of international rules, norms and principles of responsible behaviour of States:

1. States should comply with the Charter of the United Nations and universally recognized norms governing international relations that enshrine, inter alia, respect for the sovereignty, territorial integrity and political independence of all States, respect for human rights and fundamental freedoms and respect for the diversity of history, culture and social systems of all countries.

2. Consistent with the purposes of the United Nations, including to maintain international peace and security, States should cooperate in developing and applying measures to increase stability and security in the use of information and communications technologies and to prevent practices relating to such technologies that are acknowledged to be harmful or that may pose threats to international peace and security.

3. States should not use information and communications technologies and information and communications networks to carry out activities which run counter to the task of maintaining international peace and security.

4. States should not 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, and reaffirm the right and duty of States to combat, within their constitutional prerogatives, the dissemination of false or distorted news, which can be interpreted as interference in the internal affairs of other States or as being harmful to the promotion of peace, cooperation and friendly relations among States and nations.

5. States should recognize 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.

6. States should endeavour to ensure at all levels of the supply chain the security of information and communications technology goods and services, in order to prevent other States from exploiting their dominant position in information and communications technologies, including dominance in resources, critical infrastructures, core technologies, information and communications technology goods and services and information and

communications networks, to undermine the right of States to independent control of information and communications technology goods and services, or to threaten their political, economic and social security.

7. States should reaffirm the rights and responsibilities of all States, in accordance with the relevant norms and rules, regarding legal protection of their information space and critical information infrastructure against damage resulting from threats, interference, attack and sabotage.

8. States should recognize that the rights of an individual in the offline environment must also be protected in the online environment; and fully respect rights and freedoms in the information space, including the right and freedom to seek, receive and impart information, taking into account the fact that article 19 of the International Covenant on Civil and Political Rights[4] attaches to that right special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:

(a) For respect of the rights or reputations of others;

(b) For the protection of national security or of public order (ordre public), or of public health or morals;

9. All States must play the same role in, and carry equal responsibility for, international governance of the Internet, its security, continuity and stability of operation, and its development in a way which promotes the establishment of multilateral, transparent and democratic international Internet governance mechanisms which ensure an equitable distribution of resources, facilitate access for all and ensure the stable and secure functioning of the Internet.

10. States must meet their international obligations regarding internationally wrongful acts attributable to them under international law. However, 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. States should note that accusations of organizing and implementing wrongful acts brought against States should be substantiated. In case of information and communications technology incidents, States should consider all relevant information, including the larger context of the event, the challenges of attribution in the information and communications technology environment and the nature and extent of the consequences.

11. States should not knowingly allow their territory to be used for internationally wrongful acts using information and communications technologies. States must not use proxies to commit internationally wrongful acts using information and communications technologies and should seek to ensure that their territory is not used by non-State actors to commit such acts.

12. States should consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of information and communications technologies and curb the dissemination of information that incites terrorism, separatism or extremism or that inflames hatred on ethnic, racial or religious grounds, and implement other cooperative measures to address such threats. States may need to consider whether new measures need to be developed in this respect.

[4] See resolution 2200 A (XXI), annex.

13. States, in ensuring the secure use of information and communications technologies, should respect Human Rights Council resolutions 20/8 of 5 July 2012[5] and 26/13 of 26 June 2014[6] on the promotion, protection and enjoyment of human rights on the Internet, as well as General Assembly resolutions 68/167 of 18 December 2013 and 69/166 of 18 December 2014 on the right to privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression.

14. A State should not conduct or knowingly support information and communications technology activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public.

15. States should take appropriate measures to protect their critical infrastructure from information and communications technology threats, taking into account General Assembly resolution 58/199 of 23 December 2003 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures, and other relevant resolutions.

16. States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious acts using information and communications technologies. States should also respond to appropriate requests to mitigate malicious information and communications technology activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty.

17. States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of information and communications technology products, and the right of States to independent control of information and communications technology goods and services should not be undermined or their political, economic and social security threatened.

18. States should seek to prevent the proliferation of malicious information and communications technology tools and techniques and the use of harmful hidden functions.

19. States should encourage responsible reporting of information and communications technology vulnerabilities and share associated information on available remedies for such vulnerabilities to limit and possibly eliminate potential threats to information and communications technologies and infrastructure dependent on such technologies.

20. States should not conduct or knowingly support activity to harm the information systems of the authorized emergency response teams (sometimes known as computer emergency response teams or cybersecurity incident response teams) of another State. A State should not use authorized emergency response teams to engage in malicious international activity.

21. States should encourage the private sector and civil society to play an appropriate role to improve security of and in the use of information and communications technologies, including supply chain security for information and communications technology products and services. States should cooperate with the private sector and the organizations of civil society in the sphere of

[5] See *Official Records of the General Assembly, Sixty-seventh Session, Supplement No. 53* and corrigendum (A/67/53 and A/67/53/Corr.1), chap. IV, sect. A.

[6] Ibid., *Sixty-ninth Session, Supplement No. 53* (A/69/53), chap. V, sect. A.

implementation of rules of responsible behaviour in information space with regard to their potential role.

22. States should develop confidence-building measures aimed at increasing predictability and reducing the likelihood of misunderstanding and the risk of conflict. Such measures will include, inter alia, voluntary exchange of information regarding national strategies and organizational structures for ensuring a State's information security, the publication of white papers and exchanges of best practice, wherever practical and advisable.

23. States should assist developing countries in their efforts to enhance capacity-building on information security and to close the digital divide.

24. States should bolster bilateral, regional and international cooperation, promote a prominent role for the United Nations in areas such as encouraging the development of international legal norms for information security, peaceful settlement of international disputes, qualitative improvements in international cooperation in the field of information security; and to enhance coordination among relevant international organizations.

25. States should settle any dispute resulting from the application of the present set of international rules, norms and principles of responsible behaviour of States through peaceful means and refrain from the threat or use of force;

2. *Calls upon* Member States to promote further, at multilateral levels, the consideration of existing and potential threats in the field of information security, as well as possible strategies to address the threats emerging in this field, consistent with the need to preserve the free flow of information;

3. *Considers* that the purpose of such measures could be served through further examination of relevant international concepts aimed at strengthening the security of global information and telecommunications systems;

4. *Invites* all Member States, taking into account the assessments and recommendations contained in the reports of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security,[1] to continue to inform the Secretary-General of their views and assessments on the following questions:

(a) General appreciation of the issues of information security;

(b) Efforts taken at the national level to strengthen information security and promote international cooperation in this field;

(c) The content of the concepts mentioned in paragraph 3 above;

(d) Possible measures that could be taken by the international community to strengthen information security at the global level;

5. *Requests*, with a view to making the United Nations negotiation process on security in the use of information and communications technologies more democratic, inclusive and transparent, the Secretary-General, with the assistance of an open-ended working group, to be established in 2019 and acting on a consensus basis, to continue, as a priority, to further develop the norms, rules and principles of responsible behaviour of States listed in paragraph 1 above, and the ways for their implementation; if necessary, to introduce changes to them or elaborate additional rules of behaviour; to study the possibility of establishing regular institutional dialogue with broad participation under the auspices of the United Nations; and to continue to study, with a view to promoting common understandings, existing and potential threats in the sphere of information security and possible cooperative measures to address them and how international law applies to the use of information

and communications technologies by States, as well as confidence-building measures and capacity-building and the concepts referred to in paragraph 3 above, and to submit a report on the results of the study to the General Assembly at its seventy-fifth session, and to provide the possibility of holding, from within existing resources and voluntary contributions, intersessional consultative meetings with the interested parties, namely business, non-governmental organizations and academia, to share views on the issues within the group's mandate;

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