Unofficial translation

UPDATED CONCEPT OF THE CONVENTION OF THE UNITED NATIONS ON ENSURING INTERNATIONAL INFORMATION SECURITY

Information and communications technologies are dual-use technologies *(A/RES/75/240, PP8)* by their nature. They can potentially be used for purposes that are inconsistent with the objectives of maintaining international peace, security and stability and may adversely affect the integrity of the infrastructure of States to the detriment of their security in both civil and military fields *(A/RES/76/19, PP5)*. A number of States are developing information and communications technology capabilities for military purposes *(A/RES/76/19, PP3)*. The use of these technologies in future conflicts between States is becoming more likely *(A/RES/76/19, PP3)*.

There is a growing need for the peaceful use of information and communications technologies, as well as for their use for the common good of humankind and further social and economic development of all States.

There is a growing need for States to conclude a legally binding multilateral treaty within the United Nations *(A/75/816, A/76/135, A/RES/76/19, PP10)* to ensure the prevention and settlement of inter-State conflicts in the global information space, to promote the entirely peaceful use of information and communications technologies and to provide a framework for cooperation among States for these purposes.

The solution to this problem is seen in adopting the UN Convention on Ensuring International Information Security (hereinafter – the Convention), regulating the relations of States on security of and in the use of information and communications technologies. The document could include the following provisions based, among others, on the recommendations of the annual UN General Assembly resolutions entitled "Developments in the field of information and telecommunications in the context of international security", as well as the consensus reports of the relevant UN Open-Ended Working Group (OEWG) of 2021 and the Groups of governmental experts of 2010, 2013, 2015 and 2021.

I. Purposes of the Convention

The adoption of the Convention would contribute to establishing a system of international information security based on equitable cooperation between States in the field of security in the use of information and communications technologies in order to achieve the following objectives:

1. to prevent and settle inter-State conflicts in the global information

space, which pose or exacerbate a threat to international peace and security and which may undermine peace or provoke acts of aggression *(A/RES/75/240, PP10)*;

2. to build trust and develop cooperation among UN Member States in the field of international information security to overcome tensions stemming from the malicious use of information and communications technologies *(A/RES/75/240, OP1)*;

3. to support capacity-building of States in the field of security in the use of information and communications technologies *(A/RES/75/240, OP1)*.

II. Main threats to international information security and related factors

When drafting the Convention, it is appropriate to take into consideration the following threats to international information security:

1. Using information and communications technologies by States in military and political as well as other spheres in order to undermine or infringe upon the sovereignty, violate the territorial integrity, social and economic stability of sovereign States, interfere in their internal affairs, as well as to commit other acts in the global information space impeding the maintenance of international peace and security *(2021 OEWG Chair's summary, A/75/816, para 20; 2021 GGE report, A/76/135, para 70; 2015 GGE report, A/70/174, para 71 (c); contributions of China, Iran, Non-Aligned Movement to 2021 OEWG Chair's Summary, A/75/816; SCO International code of conduct for information security, A/69/723, para 3)*;

2. Carrying out computer attacks on the information resources of States, including critical information infrastructure *(2022 OEWG progress report, A/77/275, para 10; 2021 GGE report)*;

3. Monopolizing of the information and communications technology market by individual States and/or, with their assistance, by private companies through restricting access to advanced information and communications technologies to other States and increasing their technological dependence on States dominating in the field of informatization as well as increasing the digital divide *(SCO International code of conduct for information security, A/69/723, para 5)*;

4. Laying unsubstantiated accusations by some States against other States of organizing and carrying out wrongful acts with the use of information and communications technologies, including computer attacks *(2021 OEWG*

Chair's summary, A/75/816, para 15; 2021 GGE report, A/76/135, para 71 (g); 2015 GGE report, A/70/174, para.28 (f));

5. Using information resources under the jurisdiction of another State without the approval of the competent bodies of that State;

6. Placing in information space of States free-to-access tools for computer attacks, instructions on methods of their organization, coordination and development of practical skills to use such tools;

7. Using information and communications technologies to the detriment of fundamental human rights and freedoms in information space, primarily, the right to respect for private life *(A/RES/73/27, OP 1.5; 2015 GGE report, A/70/174, para 13 (e))*;

8. Integrating undeclared capabilities in information and communications technologies, as well as concealing by manufacturers of information on vulnerabilities in their products *(A/RES/73/27, OP 1.10, 1.11; 2015 GGE report, A/70/174, para 13 (i, g))*;

9. Using their own information infrastructure by States to commit internationally wrongful acts, as well as using proxies by States, including non-State actors, to commit such acts *(A/RES/73/27, OP1.13; 2015 GGE report, A/70/174, para 13 (c))*;

10. Disseminating information through information and communications technologies that is detrimental to the socio-political and socio-economic foundations, spiritual, moral and cultural environment of States and is threatening the lives and safety of citizens.

11. Inability of identifying promptly and accurately the source of computer attacks aimed at committing wrongful acts, caused by the technological specificities of information and communications technologies and the absence of institutional mechanisms to ensure de-anonymization in information space.

III. Prevention and resolution of international conflicts in the global information space

The following principles and proposals could form the basis of the provisions of the Convention related to regulating the activities of States and defining their rights and obligations in terms of preventing and resolving conflicts in the global information space:

1. the sovereign right of each State to ensure security of national information space and to establish norms and mechanisms in order to manage

its information and cultural space in accordance with national legislation *(A/RES/73/27, PP 16, 18; A/RES/75/240, PP 17, 19);*

2. sovereign equality as well as equal rights and obligations of States in the international information security system regardless of economic, social, political or other differences *(A/RES/75/240, PP17, 19; 2021 GGE Report, A/76/135, paras 70, 71 (b))*;

3. refraining in international relations from the threat or use of force against another State's information and communication infrastructure or as a means of conflict resolution *(A/RES/73/27, PP16; A/RES/75/240, PP17; contributions of Iran and China to the 2021 OEWG Chair's summary, A/75/816);*

4. prohibiting the use of information and communication technologies with a view to undermine and infringe upon the sovereignty, territorial integrity and independence of States *(2021 OEWG Chair's summary, A/75/816, para 20; 2021 GGE Report, A/76/135, para 70)*;

5. rejection of the use of information and communications technologies in order to interfere in internal affairs of sovereign States *(2015 GGE report, A/70/174, para 71 (c); contributions of Iran and China to the 2021 OEWG Chair's summary, A/75/816; SCO International code of conduct for information security, A/69/723, para 3);*

6. inadmissibility of unsubstantiated accusations of other States of committing wrongful acts with the use of information and communications technologies, including computer attacks, in particular, with a view to impose restrictions, such as sanctions and other means *(2021 OEWG Chair's summary, A/75/816, para 15; 2021 GGE Report, A/76/135, para 71 (g); 2015 GGE report, A/70/174, para 28 (f))*;

7. settlement of interstate conflicts through negotiations, mediation, reconciliation, or other peaceful means of State's choice, including through consultations with national bodies of States authorized to detect, prevent and respond to computer attacks and computer incidents *(2021 GGE report, A/75/816, para 35);*

8. Full and conscientious implementation by States of their commitments on ensuring international information security *(contribution of Canada to the 2021 OEWG Chair's summary, A/75/816)*;

9. refraining from adopting doctrines and plans aimed at provoking the escalation of threats and conflicts in the global information space, as well as at causing tensions in relations between States *(contribution of Canada to the 2021 OEWG Chair's Summary, A/75/816)*;

10. establishment by States of mechanisms to prevent computer attacks incoming from their territories or with the use of the information infrastructure under their jurisdiction, as well as to provide cooperation between States to identify the source of computer attacks carried out from their territories, counter such attacks and mitigate their consequences *(2021 OEWG Chair's summary, A/75/816, para 20; 2021 GGE report, A/76/135, paras 22, 23)*;

11. inadmissibility of bringing by States and/or with their assistance of undeclared capabilities in information and communications technologies, as well as withholding by manufacturers information on vulnerabilities of their products *(A/RES/73/27, OP 1.10, 1.11; 2015 GGE report, A/70/174, para 13 (i, g))*;

12. inadmissibility of attributing a particular activity in the field of information and communications technologies to a State solely on the basis of the origin of that activity from the territory or information infrastructure facilities of this State; the need to substantiate accusations against States of organizing and committing unlawful acts (along with that States should examine all relevant information in case of incidents, including the broader context of the event, issues with regard to establishing responsibility, the nature and scope of this responsibility) *(A/RES/73/27, OP 1.2; 2021 GGE report, A/76/135, para 71 (g); 2015 GGE report, A/70/174, para 13 (b))*;

13. inadmissibility of intentional use of their territories by States to commit internationally wrongful acts through the information and communications technologies and the engagement of intermediaries, as well as seeking to prevent non-State actors from using States' territories to commit such acts *(A/RES/73/27, OP 1.13; 2015 GGE report, A/70/174, para 13 (c))*;

14. inadmissibility of States' intentional engagement in and support of activities in the use of information and communications technologies, if such activities contradict their obligations under international law, intentionally damage critical infrastructure, or otherwise impede the use and operation of critical infrastructure to serve the public *(A/RES/73/27, OP 1.6; 2015 GGE report, A/70/174, para 13 (f))*;

15. importance of taking by States appropriate measures to protect their critical infrastructure from threats in the use of information and communications technologies *(A/RES/73/27, OP 1.7; 2015 GGE report, A/70/174, para 13(g))*;

16. refraining from using knowingly and supporting activities intented to harm the information systems of authorized computer incident response teams of another State, as well as from using authorized computer incident

response teams to conduct malicious international activities *(A/RES/73/27, OP1.12, 2015GGE report, A/70/174, para. 13 (k))*;

17. promoting the role of the private sector and civil society in enhancing security of and in the use of information and communications technologies, including the security of the entire system of production and distribution of goods and services in the field of information and communications technologies as well as information security *(A/RES/73/27, OP 1.13)*;

18. ensuring awareness of citizens, public and state bodies, relevant structures and international organizations about new threats to international information security and available options to prevent them, as well as improving literacy of all users in the field of information security;

19. refraining from using information and communications technologies and means to the detriment of fundamental human rights and freedoms exercised in information space, primarily of the human right to respect for private life *(A/RES/73/27, OP 1.5; 2015 GGE report, A/70/174, para 13(e))*;

20. respect for the free expression of views of every person, including freedom to seek, receive and disseminate information, with the possibility of imposing restrictions in accordance with the legislation in order to protect the rights and reputations of others as well as to protect the national security, public order, public health or morals *(SCO International code of conduct on information security, A/69/723, para 7; International Covenant on Civil and Political Rights, Article 19.2, Universal Declaration of Human Rights);*

21. Abstaining from any smear campaign, vilification or hostile propaganda for the purpose of interfering in the internal affairs of other States *(A/RES/73/27, PP 20; A/RES/75/240, PP 21)*.

IV. Confidence-building and promoting cooperation in the field of international information security

The following principles and proposals could form the basis for the provisions of the Convention governing the activities of States and defining their rights and obligations with regard to the implementation of confidence-building and cooperation in the field of international information security:

1. recognizing that developing international cooperation on security of and in the use of information and communications technologies will improve overall security as well as the effectiveness of responses to related threats (OEWG 2021 report, A/75/816, paras. 3, 5; GGE 2021 report, A/76/135,

para. 5);

2. the exchange of national legislation on security of and in the use of information and communications technologies (OEWG 2022 progress report, A/77/275, section D, recommendation 3; GGE 2021 report, A/76/135, paras. 83, 84);

3. prompt exchange of information on crisis and threats in the information space and measures taken with respect to their regulation and neutralization (OEWG 2022 progress report, A/77/275, para. 16(c); GGE 2021 report, A/76/135, para. 83; GGE 2015 report, A/70/174, para. 13(j));

4. prompt exchange of information on computer incidents and computer attacks committed against States, noting that States may develop a standardized set of technical information to be transmitted to respond to those threats (GGE Report 2021, A/76/135, para. 63);

5. holding consultations on activities in information space that may be of concern to prevent and resolve conflicts in information space peacefully (GGE Report 2021, A/76/135, paras. 23, 25);

6. developing mechanisms for sharing best practices in responding to threats to international information security (OEWG Report 2021, A/75/816, paras. 22, 43).

V. Promoting national capacity-building in the field of security in the use of information and communications technologies

The following principles and proposals could serve as the basis for the provisions of the Convention governing State activities and defining the rights and obligations of States with regard to promoting State capacity-building in the field of security in the use of information and communications technologies:

1. promoting cooperation between States in the field of international information security to maintain international peace and security (OEWG Report 2021, A/75/816, para. 3);

2. assisting States in their efforts to build security capacity in the use of information and communication technologies at the request of each recipient State and according to its needs and characteristics (A/RES/77/36, PP5, OP6; A/RES/75/240, PP21; OEWG Report 2021, A/75/816, para. 56);

3. development of universal principles and programmes to assist developing countries in building their capacity in the field of security in the use of information and communications technologies under the United Nations auspices (OEWG Report 2021, A/75/816, para. 56);

4. development of public-private partnerships *(2021 OEWG Report, A/75/816, para. 18)*;

5. promotion of the development and use of secure information and communications technologies in compliance with the principle of neutrality of the global communications network, including the evolutionary reforming of protocols and information transfer methods to eliminate the possibility of using this network for criminal purposes;

6. inadmissibility of the use by individual States and/or private companies with their assistance of technological dominance to monopolize the information and communications technologies market, limit the access of other States to cutting-edge information and communications technologies, including main information resources, critical infrastructure, key technologies, products and services, as well as increase the technological dependence of States and prevent them from exercising independent control and carrying out measures to ensure information security *(2021 OEWG Report, A/75/816, para.11; China's contribution to the 2021 OEWG Chair's Summary, A/75/816*; *SCO code of conduct for information security, A/69/723, para.5)*;

7. prevention of discrimination in trade and economic activities that involve information and communications technologies through a just distribution of income from such activities that would facilitate the strengthening of States' national capacities to ensure international information security *(2021 OEWG Report, A/75/816, para.11; China's contribution to the 2021 OEWG Chair's Summary, A/75/816);*

8. inadmissibility of misuse of information and communications technologies supply chains developed under the control and jurisdiction of States by creating vulnerabilities in products, goods and services at the expense of the sovereignty and data security of individual States *(2021 OEWG Report, A/75/816, para. 28; China's and Iran's contributions to the 2021 OEWG Chair's Summary, A/75/816);*

9. inadmissibility of undue restrictions against States, including unilateral coercive measures that prevent universal access to the benefits of peaceful uses of information and communications technologies, international cooperation or transfer of such technologies *(2021 OEWG Chair's Summary, A/75/816, para. 24; Non-Aligned Movement's contribution to the 2021 OEWG Chair's Summary, A/75/816).*

VI. Mechanisms for the development and implementation of the Convention

The draft Convention should be developed under the United Nations auspices taking into account the opinions of all Member States within the framework of a negotiation mechanism that should be established for this purpose.

In accordance with the generally accepted practice of concluding multilateral international treaties, the future Convention should include mechanisms to verify the implementation of its provisions by States, to amend and supplement it, to exchange views on its implementation, as well as to settle and peacefully resolve disputes. The verification mechanism should operate under the United Nations auspices while respecting the principles of its Charter, including, above all, the sovereign equality of States. Existing examples include: permanent bodies with the participation of all States that joined the Convention and regular review conferences. The specific parameters of this mechanism should be defined in the process of negotiating the draft Convention.