CONCEPT OF UN CONVENTION ON INTERNATIONAL INFORMATION SECURITY

PREAMBLE

We note considerable progress in the development of information and communications technologies and means that build information space,

Express our concern about threats related to possible uses of these technologies and means for purposes inconsistent with the objectives of ensuing international peace, security and strategic stability,

Attach importance to preventing conflicts in information space and to establishing effective global, regional, multilateral and bilateral cooperation in this area, and also *note* in this context United Nations General Assembly resolutions A/RES/68/243 of 27 December 2013, A/RES/69/28 of 2 December 2014, A/RES/70/237 of 23 December 2015, A/RES/71/28 of 5 December 2016, A/RES/73/27 of 5 December 2018, A/RES/74/29 of 12 December 2019 and A/RES/75/240 of 31 December 2020 “Developments in the field of information and telecommunications in the context of international security” that contribute to progress in this issue,

Attach importance to building an international information security system as one of the key elements of the entire international security system, aimed at ensuring global stability amidst growing dependence of the information society on information and communications technologies,

Strongly believe that further increased confidence and development of cooperation among States Parties in ensuring international information security are an objective necessity and serve their interests,

Take into consideration the important role of information security in enjoyment of human rights and fundamental freedoms, primarily of right to respect for private life and protection of personal data,

Desire to create a legal and organizational framework for cooperation among States Parties in ensuring international information security,

Refer to the United Nations General Assembly resolution A/RES/55/29 of 20 December 2000 "Role of science and technology in the context of international security and disarmament", which, in particular, recognizes that scientific and technological developments can have both civilian and military applications and that progress in science and technology for civilian applications needs to be maintained and encouraged,

Recognize the need to prevent possible threats of the use of information and communications technologies for purposes inconsistent with ensuring strategic stability and international information security, and that may affect the integrity of digital infrastructures, undermining their security, *Stress* the need for enhanced coordination and reinforced cooperation between States in countering wrongful use of information and communications technologies for military and political, terrorist and criminal purposes,

Note the leading role of the United Nations in ensuring information security of States Parties and in building a secure global information space, as well as the importance of the activities of other international and regional organizations,

Underline the importance of developing a common understanding and of ensuring international cooperation on an equitable basis in the interests of secure, uninterrupted and stable operation of the Internet and other information and communications networks and their protection against possible threats,

Reaffirm that political authority related to the Internet is a sovereign right of States, and that States have rights and responsibilities with regard to such issues at the international level,

Note the need to intensify efforts to overcome the "digital divide" through ensured access of developing countries to information and communications technologies and build-up of their capacities concerning best practices and advanced training in the field of ensuring security in the use of these technologies,

Strongly believe in the need for States to implement policies aimed at protecting their citizens against wrongful acts in information space, including through adoption of relevant legislation and strengthened international cooperation,

Express concern about the threat that information and communications networks, including the Internet, may also be used to commit wrongful acts, and *take into account* that “digital” evidence of such acts is kept in these networks,

Recognize the need for cooperation between governments and business circles in combatting wrongful acts in information space and for protection of their legal interests in the field of the use and development of information and communications technologies,

Believe that effective fight against wrongful acts in information space requires more extensive, dynamic and well-established international cooperation, and in this context *note* the United Nations General Assembly resolution A/RES/74/247 of 27 December 2019 “Countering the use of information and communications technologies for criminal purposes” and the establishment under the resolution of an open-ended ad hoc intergovernmental committee of experts to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes,

Assume that it is necessary to ensure an appropriate balance between the human right to freedom of expression, including freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his/her choice, under the 1966 International Covenant on Civil and Political Rights and special duties and responsibilities related to the enjoyment of the mentioned rights, which may be subject to certain restrictions that are established by law and are necessary for respect of the rights or reputations of others, for the protection of national security, public order, or public health or morals, envisaged by the same Covenant,

Welcome the willingness of States to further enhance mutual understanding, confidence and cooperation to ensure international information security, including efforts of the United Nations, the Shanghai Cooperation Organization, BRICS, the Commonwealth of Independent States, the European Union, the Council of Europe, the Organization for Security and Cooperation in Europe, the Asia-Pacific Economic Cooperation Forum, the Central American Integration System, the Organization of American States, the Association of Southeast Asian Nations, the African Union, and other international organizations and fora.

GENERAL PROVISIONS

Objectives of the Convention

Contribute to building an international information security system that ensures countering threats to international peace, security and strategic stability in information space and facilitates:

a) Equitable strategic partnership in global information space on the basis of sovereign equality of States;

b) Overall social and economic development on the basis of equal and secure access of all States to modern ICT developments;

c) Implementation of universally recognized principles and norms of international law, including principles of peaceful settlement of disputes and conflicts, non-use of force, non-interference in internal affairs, and respect for human rights and fundamental freedoms;

d) Exercise of everyone’s right to seek, receive and impart information and ideas of all kinds, taking into account that this right may be subject to certain restrictions established by law and necessary for respect of the rights or reputations of others, as well as for the protection of national security, public order, public health or morals;

e) Free exchange of technology and information with respect for the sovereignty of States and their existing political, legal, historical and cultural specificities.

Main threats and factors affecting international information security

1. Use of information and communications technologies for military and political purposes contrary to international law for hostile activities and acts of aggression aimed at discrediting the sovereignty and violating the territorial integrity of States and posing a threat to international peace, security and strategic stability.

2. Use of information and communications technologies for terrorist purposes, including for computer attacks on information infrastructure facilities, as well as for propaganda of terrorism and engagement of new supporters in terrorist activities.

3. Use of information and communications technologies to interfere in internal affairs of sovereign States, disturb public order, incite national, racial or religious enmity, disseminate racist and xenophobic ideas or theories giving rise to hatred and discrimination and inciting violence, or to undermine social and political and socio-economic systems, as well as spiritual, moral or cultural environment of States.

4. Use of information and communications technologies to commit crimes, including those related to illegal access to computer information, and creation, use and dissemination of harmful software.

5. Use of information resources under the jurisdiction of another State without the consent of the competent bodies of that State.

6. Dissemination of harmful software and information contrary to the principles and norms of international law and national legislations.

7. Use of 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.

8. Disruption of the secure, uninterrupted and stable functioning of the Internet.

9. Prevention of access to latest information and communications technologies and creation of conditions of technological dependence in the field of information.

10. Inclusion of undeclared capabilities in information and communications technologies, as well as withholding by manufacturers of information on vulnerabilities of their products.

11. Inadequate assessment of emerging threats to information security related to introduction of new technologies, such as artificial intelligence, big data, Internet of Things, blockchain, etc.

12. Use of technological dominance to monopolize various segments of the information and communications technologies market, including main information resources, critical infrastructure, key technologies, products and services, as well as to impede independent control and measures to ensure information security.

13. State-approved use of their information infrastructure to commit internationally wrongful acts, as well as use of proxies by States, including non-State actors, to commit such acts.

14. Public dissemination of knowingly false information under the guise of credible messages leading to a threat to life or safety of citizens or to serious consequences.

15. Inability to precisely identify the source of computer attacks or false information due to technological specificities of information and communications technologies and absence of organizational mechanisms to ensure de-anonymization of information space.

Main principles of ensuring international information security

1. Consistency with the objectives of maintaining international peace, security and strategic stability.

2. Compliance with universally recognized principles and norms of international law, including the principles of peaceful settlement of disputes and conflicts, non-use of force in international relations, non-interference in internal affairs of other States, and respect for the sovereignty of States and for human rights and fundamental freedoms.

3. Indivisibility of security meaning that the security of each State is inseparable from the security of all other States and should be ensured without detriment to the security of other States.

4. Adequate capacity of any State to ensure the security of its national information space.

5. Sovereign equality and equal rights and responsibilities of States irrespective of economic, social, political or any other differences.

6. Possibility of establishing sovereign norms and mechanisms to manage its information space under the national legislation.

7. Freedom and independence in pursuing its sovereign interests in information space and freedom in selecting ways of ensuring its information security under international law.

8. Settlement of conflicts via negotiations, mediation, reconciliation, resort to relevant regional bodies or other peaceful means of a State’s choice in a manner avoiding threat to international peace and security.

9. Applicability of the inalienable right to self-defense against aggression in information space provided that the source of aggression is clearly identified and response measures are adequate and take into account norms of international humanitarian law.

10. Inadmissibility of unsubstantiated and ill-founded accusations of other States in committing wrongful acts with the use of information and communications technologies, including computer attacks, *inter alia* with a view to imposing follow-up penalties of various kinds, such as sanctions and other responses.

11. Respect for fundamental civil rights and freedoms, including protection against unauthorized interference in private life of citizens while maintaining the balance between those rights and the objectives to counter the use of information space for terrorist and other criminal purposes.

12. Inadmissibility of restrictions or violation of access to information space, except for purposes of protection of the constitutional order foundations, morality, health, rights and legitimate interests of other persons, and of ensuring the country’s defense and the security of the State.

13. Inadmissibility of trans-border access to computer information stored in the information system of another State without official interaction with law-enforcement bodies of this State.

14. Good will and reciprocity in prevention, detection, suppression, solving and investigation of wrongful acts in the field of use of information and communications technologies, including for terrorist and other purposes, and mitigation of consequences of such acts.

PREVENTION OF CONFLICTS IN INFORMATION SPACE

Main measures of prevention of conflicts in information space

1. Cooperation in the field of ensuring information security to maintain international peace and security, and international economic stability.

2. Creation by States of mechanisms to prevent destructive information impact (computer attacks) from their territories or with the use of the information infrastructure under their jurisdiction and to cooperate to identify the source of computer attacks from their territories, counter such attacks and mitigate their consequences.

3. Refraining from drafting and adopting doctrines and plans that may provoke escalation of threats and emergence of conflicts in information space and also cause tensions in relations between States.

4. Refraining from any actions threatening the security of information space of another State.

5. Non-use of information and communications technologies to interfere in affairs under the internal competence of another State.

6. Refraining from organization or encouragement of organization of any irregular forces to commit any wrongful acts in information space of another State.

7. Countering the dissemination of false or distorted information provided the non-discriminatory access to resources.

8. Countering the creation, dissemination and application of technologies and means to commit illegal activities with the use of information and communications technologies.

9. Countering the development, dissemination and use of harmful software.

10. Prevention of any unauthorized interference in the operation of international information systems of management of traffic and financial flows, means of communication, means of international information exchanges, including academic and educational ones.

11. 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 modes of communication of information to exclude the possibility of the use of this network for criminal purposes.

12. Ensuring the security of legally protected information, including intellectual property, trademarks and copyrights.

13. Encouragement of public-private partnership to decrease threats to information security and increase the level of security.

14. Ensuring awareness of citizens, public and State bodies, relevant structures and international organizations about new threats in information space and known ways to neutralize them, and higher literacy of all users in the field of information security.

COUNTERING THE USE OF INFORMATION SPACE FOR TERRORIST PURPOSES

Main measures of countering the use of information space for terrorist purposes

1. Coordination of actions to prevent any terrorist activity with the use of information and communications technologies.

2. Expeditious exchange of information on signs, facts, methods and modes of use of information space for terrorist purposes, including through computer attacks, as well as mutual reporting on legal regulation and organization of activities to counter those wrongful acts, on gained experience and practice in this field.

3. Improvement of legislation to organize activities of law-enforcement and other bodies to counter and suppress the use of information space for terrorist purposes.

COUNTERING THE USE OF INFORMATION AND COMMUNICATIONS TECHNOLOGIES FOR CRIMINAL PURPOSES

Criminally punishable acts in the field of the use of information and communications technologies

1. Destruction, blocking, modification or copying of information, disruption of work of the information (computer) system by means of an unauthorized access to legally protected computer information.

2. Creation, use or dissemination of harmful software.

3. Improper use of a computer system by a person with access to it leading to destruction, blocking or modification of legally protected information, if that act caused significant damage or serious consequences.

4. Larceny of property through modification of information processed in a computer system and stored in a machine medium or communicated via a data network, either via entering false information into a computer system, or larceny via an unauthorized access to legally protected information.

5. Dissemination of pornographic materials or objects with images of a minor with the use of the Internet or any other telecommunication channels.

6. Manufacturing with a view to selling or selling of special software or hardware enabling an unauthorized access to a protected computer system or network.

7. Illegal use of software for copyrighted computer systems or databases, as well as appropriation of authorship, if this act caused significant damage.

8. Dissemination with the use of the Internet of materials duly recognized as extremist or containing appeals to terrorist activity or justification of terrorism.

9. Dissemination with the use of the Internet of information containing scenes of aggression or violence and information discrediting honour and dignity of a person.

10. Wrongful influence on critical information infrastructure.

Main measures of countering the use of information and communications technologies for criminal purposes

1. Improvement of the legal framework of cooperation in countering crimes committed with the use of information and communications technologies, including relevant international bilateral and multilateral treaties, *inter alia* on legal assistance in criminal cases, and in the framework of international police cooperation, including channels of the International Criminal Police Organization – INTERPOL.

2. Development and implementation of joint programmes and plans to counter crimes committed with the use of information and communications technologies.

3. Cooperation with relevant international organizations to suppress and investigate crimes committed with the use of information and communications technologies.

4. Organization of cooperation to implement provisions of international regulatory legal documents aimed at countering crimes committed with the use of information and communications technologies.

5. Mutual legal assistance in developing national systems of measures to counter crimes committed with the use of information and communications technologies.

6. Assistance in investigative, operative and search, and other activities to counter crimes committed with the use of information and communications technologies.

7. Exchange of experience in prevention, detection, suppression, solving and investigation of crimes committed with the use of information and communications technologies, organization of joint seminars, exercises, trainings, consultations and meetings.

8. Improvement of methods and forms of interaction of competent bodies in countering crimes committed with the use of information and communications technologies, and implementation of best practices in the work of the mentioned bodies.

9. Training, requalification and skill upgrading of personnel participating in countering crimes committed with the use of information and communications technologies.

10. Joint scientific research in the field of countering crimes committed with the use of information and communications technologies.

CONFIDENCE-BUILDING MEASURES IN ENSURING INTERNATIONAL INFORMATION SECURITY

1. Exchange of national concepts of ensuring information security (security in the use of information and communications technologies).

2. Expeditious exchange of information on crisis events and threats in information space and measures taken to address and neutralize them.

3. Exchange of information on computer incidents and computer attacks committed against States, taking into account that amount of such information is to be determined by the States.

4. Consultations on activities in information space that may cause concern with a view to preventing and peacefully settling conflicts in information space.

5. Exchange of information on measures to ensure free, secure and stable operation of the Internet.

6. Development of public-private partnerships and mechanisms of exchange of best practices of responding to threats to international information security.

Source: http://www.scrf.gov.ru/security/information/Concept_en/