INTERNATIONAL MEETING of HIGH-RANKING OFFICIALS
RESPONSIBLE for SECURITY MATTERS

CONVENTION

on INTERNATIONAL INFORMATION SECURITY

(CONCEPT)

EKATERINBURG, RUSSIA,

21-22 SEPTEMBER 2011

CONVENTION
ON INTERNATIONAL INFORMATION SECURITY
(Concept)

PREAMBLE

The States Parties to the Convention,

noting the considerable progress in the development of information and communication technologies and means that make up the information space,

expressing their concerns about threats connected with the possible uses of these technologies and means for purposes not compatible with measures to ensure international security and stability, both in the military and the civilian spheres,

understanding the importance of international information securiy as one of the key elements in the system of internationl security,

confident that the further growth of trust and the development of cooperation between the States Parties on issues of international information security are essential and beneficial to all parties,

taking into consideration the important role that information security plays in ensuring basic human rights and freedoms,

taking into account the 8 December 2010 resolution A/RES/65/41 of the General Assembly of the United Nations "Developments in the field of information and telecommunications in the context of international security",

striving to limit threats to international information security, ensure the information security of States Parties, and create an information space characterized by peace, cooperation, and harmony,

desiring to create a legal and organizational basis for cooperation between the States Parties in the sphere of international information security,

referring to the 20 November 2000 resolution A/RES/55/29 of the General Assembly of the United Nations "Role of science and technology in the context of international security and disarmament", in which, in part, it is stated that achievements in science and technology can be put to both civilian and military use, and that it is necessary to support and stimulate the development of science and technology for use in civilian activities,

acknowledging the necessity of preventing possible uses of information and communication technology for purposes not compatible with ensuring international stability and security, and capable of having a negative effect on the integrity of governmental infrastructures, causing damage to their security,

stressing the necessity of increasing the coordination and strengthening the cooperation between States in the struggle against the criminal use of information technology and noting the role the United Nations and other international and regional organizations can play in that context,

stressing the importance of the secure, uninterrupted, and stable functioning of the Internet and the necessity of protecting the Internet and other information and communication networks from possible harmful actions vulnerability to threats,

affirming the necessity for a common understanding of Internet security issues and further cooperation on the national and international level,

affirming again that political authority in connection with governmental policy issues related to the Internet is a sovereign right of States, and that the governments of States have rights and responsibilities as regards governmental policy issues related to the Internet on an international level,

acknowledging that trust and security when using information and communication technologies is a fundamental basis of the information society, and that it is necessary to stimulate, form, develop, and actively integrate a stable global culture of cybersecurity, as is noted in the 21 December 2009 resolution A/RES/64/211 of the General Assembly of the United Nations “Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures”,

noting the necessity of activating efforts to overcome the “digital divide” by increasing the ease of supply of information and communication technology to developing countries, and increasing their potential in relation to cutting-edge practices and professional training in the sphere of cybersecurity, as is noted in the 21 December 2009 resolution A/RES/64/211 of the General Assembly of the United Nations “Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures”,

convinced of the necessity of prioritizing the creation of a common policy aimed at protecting society against illegal actions in the information space, which will include passing corresponding legislation and strengthening international cooperation,

recognizing the serious changes caused by the spread of digital technology, unification, and continuing globalization of computer networks,

concerned about the threat that computer networks may also be used to commit crimes, and that the proof of such crimes may be kept in these networks and passed on within them,

acknowledging the necessity of cooperation between governments and private business in the fight against illegal activity in the information space and the necessity of protecting the legal interests of parties involved in the use and development of information and communication technology,

believing that fighting illegal activity in the information space effectively requires international cooperation that is broader, more dynamic, and more efficient,

convinced that this Convention is necessary in the fight against breeches of the confidentiality, integrity, and accessibility of computer systems and networks and computer information, as well as the misuse of such systems, networks, and information by ensuring the punishment of such actions, detailed in this Convention, and in the granting of sufficient authority to effectively fight such offenses through the tracking, exposure, and investigation of such offenses on an internal and international level, and through the development of agreements on efficient and reliable international cooperation,

keeping in mind the necessity of ensuring the appropriate balance between maintaining law and order and protecting fundamental human rights, as foreseen in the 1966 International Covenant on Civil and Political Rights, as well as other international human rights agreements, which assert the right of each individual to freely hold his or her own ideas, and to freely express these ideas and opinions, including the freedom to seek, receive, and distribute any kind of information or idea, regardless of national borders,

keeping in mind also the right to a private life and the protection of personal data,

taking into account the 1989 United Nations Convention on the Rights of the Child, and the Convention concerning the prohibition and immediate action for the elimination of the worst forms of child labour, passed by the General Conference of the International Labour Organization in 1999,

welcoming recent events enabling the further growth of international understanding and collaboration in the struggle against illegal activity in the information space, including measures undertaken by the United Nations, the

Shanghai Cooperation Organization, the European Union, the Asia-Pacific Economic Cooperation organization, the Organization of American States, the Association of Southeast Asian Nations, the Organisation for Economic Co-operation and Development, the Group of Eight (G8), and other international organizations and forums, have agreed to the following:

Chapter 1. MAIN CLAUSES

Article 1. Subject and aim of the Convention

The subject that this Convention seeks to regulate is the activity of governments to ensure international information security.

The aim of this Convention is to act against the use of information and communication technology to violate international peace and security, as well as to set up measures ensuring that the activity of governments in the information space will:

1) further general social and economic development;

2) be carried out in such a way as to be compatible with efforts to support international peace and security;

3) correspond to generally accepted principles and norms of international law, including principles of peacefully regulating conflicts and disagreements, abstaining from the use of force, not interfering in internal issues, and respecting fundamental human rights and freedoms;

4) be compatible with the right of each individual to seek, receive, and distribute information and ideas, as is affirmed in UN documents, while keeping in mind that this right may be restricted through legislation to protect the national and social security of each State, as well as to prevent the wrongful use of and unsanctioned interference in information resources;

5) guarantee the free exchange of technology and information, while maintaining respect for the sovereignty of States and their existing political, historical, and cultural specificities.

Article 2. Terms and definitions

The following terms and definitions are used for this Convention:

"**access to information**" - the possibility of receiving and using information;

"**information security**" - a state in which personal interests, society, and the government are protected against the threat of destructive actions and other negative actions in the information space;

"**information warfare**" - conflict between two or more States in the information space with the goal of inflicting damage to information systems, processes, and resources, as well as to critically important structures and other structures; undermining political, economic, and social systems; carrying out mass psychological campaigns against the population of a State in order to destabilize society and the government; as well as forcing a State to make decisions in the interests of their opponents;

"**information infrastructure**" - the total complex of technical means and systems of the formation, conversion, transfer, use, and storage of information;

"**information system**" - the total amount of information stored in a database and the technology used to support the processing of that information;

"**information weapon**" - information technology, means, and methods intended for use in information warfare;

"**information space**" - the sphere of activity connected with the formation, creation, conversion, transfer, use, and storage of information and which has an effect on individual and social consciousness, the information infrastructure, and information itself;

"**information and communication technologies**" - the total amount of methods, production processes, and programming and technical elements, integrated with the goal of forming, converting, transferring, using, and storing information;

"**information resources**" - an information infrastructure, as well as the information itself and the flow of that information;

"**confidentiality of information**" - the mandatory requirement that a party granted access to certain information will not transfer this information to a third party without the agreement of the owner;

"**critically important part of the information infrastructure**" - a part (element) of an information infrastructure, actions against which could have consequences directly connected to national security, including the security of individuals, society, and the government;

"**international information security**" - a state of international relations that excludes the possibility of breaks in global stability or the creation of threats to the security of governments and the global community in the information space;

"**the misuses of information resources**" - the use of information resources without the necessary rights, or which involves a violation of existing regulations, national legislation, or international legal norms;

"**unsanctioned interference in information resources**" - illegal action affecting the processes of forming, processing, converting, transferring, using, and storing information;

"**information system operator**" - an individual citizen or corporation whose runs an information system, including the processing of information contained in its database;

"**illegal activity in the information space**" - the use of information resources and/or activity affecting them in the information space for illegal purposes;

"**presentation of information**" - actions aimed at the receipt of information by a certain group, or the transfer of information to a certain group;

"**dissemination of information**" - actions aimed at the receipt of information by an indefinite group, or the transfer of information to an indefinite group;

"**terrorism in the information space**" - the use of information resources and/or activity affecting them in the information space for the purposes of terrorism;

"**threat to the information space (threat to information security)**" - factors that pose a danger to individuals, society, and the state, and their interests, in the information space.

Article 3. Exceptions to the application of this Convention

This Convention will not apply in those cases when the actions in question are taken within the information infrastructure of one State, citizen, or corporation under the jurisdiction of that State, and the effects of those actions are only felt by citizens and corporations under the jurisdiction of that State, and no other State has grounds to assert its jurisdiction.

Article 4. The main threats to international peace and security in the information space

The following are seen as the main threats in the information space that could damage international peace and stability:

1) the use of information technology and means of storing and transferring information to engage in hostile activity and acts of aggression;

2) purposefully destructive behavior in the information space aimed against critically important structures of the government of another State;

3) the illegal use of the information resources of another government without the permission of that government, in the information space where those resources are located;

4) actions in the information space aimed at undermining the political, economic, and social system of another government, and psychological campaigns carried out against the population of a State with the intent of destabilizing society;

5) the use of the international information space by governmental and non-governmental structures, organizations, groups, and individuals for terrorist, extremist, or other criminal purposes;

6) the dissemination of information across national borders, in a manner counter to the principles and norms of international law, as well as the national legislation of the government involved;

7) the use of an information infrastructure to disseminate information intended to inflame national, ethnic, or religious conflict, racist and xenophobic written materials, images or any other type of presenting ideas or theories that promote, enable, or incite hatred, discrimination, or violence against any individual or group, if the supporting reasons are based on race, skin color, national or ethnic origin, or religion;

8) the manipulation of the flow of information in the information space of other governments, disinformation or the concealment of information with the goal of adversely affecting the psychological or spiritual state of society, or eroding traditional cultural, moral, ethical, and aesthetic values;

9) the use, carried out in the information space, of information and communication technology and means to the detriment of fundamental human rights and freedoms;

10) the denial of access to new information and communication technologies, the creation of a state of technological dependence in the sphere of informatization, to the detriment of another State;

11) information expansion, gaining control over the national information resources of another State.

Additional factors increasing the danger of the aforementioned threats are:

1) difficulty in identifying the source of hostile actions, especially taking into account the growing activity of individuals, groups, and organizations, including criminal organizations, which provide intermediary services, carrying out activities in the name of others;

2) the potential danger of the inclusion of undeclared destructive capabilities in information and communication technology;

3) the difference in the levels of information and communication technologies in use, and in their security, in different States ("digital inequality");

4) the difference in national legislation and practices as regards the formation of a secure and quickly restorable information infrastructure.

Article 5. Main Principles of Ensuring International Information Security

The information space belongs to humankind as a whole. Its security is instrumental in ensuring the sustainable development of global civilization.

To create and foster an atmosphere of trust in the information space, the States Parties must observe the following principles:

1) the activities of each State Party in the information space must promote social and economic development and must be consistent with the goals of maintaining world peace and security, and conform to the universally recognized principles and norms of international law, including the principles of peaceful reconciliation of strife and conflict, of the non-use of force in international relations, of non-interference into the internal affairs of other States, and of respect for the sovereignty of States and the major human rights and freedoms;

2) as they shape the system of international information security, the States Parties shall be guided by the principle of indivisibility of security, which means that the security of each State is inextricably connected with the security of all other States and the international community as a whole and shall not strengthen their security at the expense of the security of other States;

3) each State Party must strive to overcome the disparity in the level of equipment of national information systems with modern information and communication technologies, to bridge the “digital divide” with the purpose of lowering the general threat level in the information space;

4) all States Parties in the information space enjoy sovereign equality, have equal rights and obligations and are possess equal rights as stakeholders in the information space irrespective of their economic, social, political and other differences;

5) each State Party has the right to make sovereign norms and govern its information space according to its national laws. Its sovereignty and laws apply to the information infrastructure located in the territory of the State Party or otherwise falling under its jurisdiction. The States Parties must strive to harmonize national legislation, the differences whereof must not create barriers on the road to a reliable and secure information space;

6) each State Party must observe the principle of responsibility for its own information space, including responsibility for its security and the nature of information it holds;

7) each State Party has the right to develop its information space without external interference and each other State must respect that right in accordance with the principle of equal rights and self-determination of peoples stipulated in the Charter of the United Nations;

8) each State Party, with consideration for the lawful interests in security of other States, may freely and independently determine its interests in the support of information security, on the basis of sovereign equality, as well as freely choose the methods by which it will ensure its own information security in accordance with international law;

9) the States Parties acknowledge that aggressive “information warfare” is a crime against international peace and security;

10) the information space of States Parties should not be the object of acquisition for other States as a result of threats of force or the use of force;

11) each State Party has the inalienable right to self-defense against aggressive actions against it in the information space, if the source of aggression can be reliably located and the retaliatory measures are appropriate;

12) each State Party will determine its military potential in the information space on the basis of national procedures, with consideration for the lawful interests in security of other States, as well as the necessity of working to strengthen international peace and security. No State Party will make an attempt to achieve dominance in the information space over other States;

13) a State Party may locate its forces and means of ensuring information security on the territory of another State in accordance with an agreement, developed by both parties on a voluntary basis through negotiations, and in accordance with international law;

14) each State Party will take the measures necessary to ensure that the activity of international information systems for the management of the flow of transport and finance, means of communication, means of international information exchange, including the exchange of information for scientific and educational purposes, continues without interference, based on the understanding that such interference could negatively affect the information space as a whole;

15) States Parties should support and stimulate scientific and technical developments connected with the exploration of the information space, as well as educational activity, aimed at forming a global culture of cybersecurity;

16) each State Party will, within the limits of its means, ensure that fundamental human rights and freedoms, and the rights and freedoms of citizens, and intellectual property laws, including patents, technologies, commercial secrets, brands, and copyrights, are adhered to in its information space;

17) each State Party guarantees freedom of speech and expression in its information space, as well as protection against illegal interference into the private lives of citizens;

18) each State Party aims to maintain a balance between fundamental human rights and the effective counteraction of terrorist use of the information space;

19) States Parties do not have the right to limit or interrupt the access of citizens to the information space, except when acting to protect national and social security, or when preventing the illegal use of an unsanctioned interference into their national information infrastructure;

20) States Parties stimulate the partnership between business and civil society in the information space;

21) States Parties acknowledge their responsibility to ensure that citizens, public and state bodies, other States, and the global community are informed about new threats to the information space and about known methods of increasing the level of their security.

Chapter 2. MAIN MEASURES FOR AVERTING AND RESOLVING MILITARY CONFLICT IN THE INFORMATION SPACE

Article 6. Main Measures for Averting Military Conflict in the Information space

Guided by the principles laid out in Article 5, the States Parties shall take steps to anticipate and expose potential conflicts in the information space and take joint action to avert them and resolve crises and disputes peacefully.

To this end, the States Parties shall:

1) cooperate to ensure international information security to maintain world peace and security and to contribute to global economic stability and progress, general welfare of the peoples of the world and discrimination-free international cooperation;

2) take all necessary steps to prevent any destructive information action originating from their own territory or using the information infrastructure under their jurisdiction, as well as cooperate to locate the source of computer attacks carried out with the use of their territory, to repel these attacks and to eliminate their consequences;

3) refrain from developing and adopting plans or doctrines capable of increasing threats in the information space, straining relations between States or provoking “information wars”;

4) refrain from any actions aimed at a complete or partial breach of the integrity of the information space of another State;

5) refrain from using information and communication technology to interfere with the internal affairs of another State;

6) refrain, in international relations, from threatening to use or using force against the information space of any other State with the purpose of breaching it or as a means of resolving conflict;

7) refrain from organizing or encouraging the organization of any irregular forces with the purpose of carrying out unlawful activities in the information space of another State;

8) refrain from slander as well as from using insulting or hostile propaganda to intervene into or interfere in the internal affairs of other States;

9) have the right and duty to take action against the proliferation of untruthful or distorted messages which could be considered as a means of interfering in the internal affairs of other States or as damaging world peace and security;

10) take action aimed at limiting the proliferation of “information weapons” and the technology for their creation.

Article 7. Measures for Resolving Military Conflict in the Information Space

1) The States Parties shall resolve conflicts in the information space primarily by means of negotiation, investigation, mediation, reconciliation, arbitration, court trial, appeal to regional bodies or agreements, or by other peaceful means of their choice so as not to endanger world peace and security.

2) In any international conflict, the right of the States Parties that are involved in the conflict to choose the means of “information warfare” is limited by applicable norms of international humanitarian law.

Chapter 3. MAIN MEASURES FOR PREVENTING THE USE OF THE INFORMATION SPACE FOR TERRORIST PURPOSES

Article 8. The Use of the Information space for Terrorist Purposes

The States Parties acknowledge the possibility of the information space being used for carrying out terrorist activities.

Article 9. Main Measures for Preventing the Use of the Information space for Terrorist Purposes

To prevent the use of the information space for terrorist purposes, the States Parties shall:

1) take action to prevent the use of the information space for terrorist purposes and acknowledge the necessity of decisive joint efforts to this end;

2) strive to work out uniform approaches to disabling Internet resources of a terrorist nature;

3) acknowledge the need for establishing and expanding the exchange of information on possible computer attacks, on the signs, facts, methods, and means of using the Internet for terrorist purposes, and on the goals and activities of terrorist organizations in the information space, as well as the need for the exchange of experience and best practices on monitoring Internet resources, finding and monitoring the content of websites of a terrorist nature, carrying out criminal investigations by computer experts in this sphere, and legal regulation and

the organization of activities for preventing the use of the information space for terrorist purposes;

4) take such steps of legislative or other nature as may be necessary to allow law enforcement authorities to carry out investigative and other relevant activities aimed at preventing and suppressing terrorist activities in the information space and at the elimination of the consequences thereof, as well as at punishing persons and organizations guilty of conducting them;

5) take necessary steps of legislative or other nature which will guarantee lawful access to specific parts of the information and communication infrastructure in the territory of the State Party, which are legally implicated in being employed for the perpetration of terrorist activities in the information space or involved in such activities elsewhere, for the perpetration of activities conducive to terrorist acts, or for the activities of terrorist organizations or groups, or individual terrorists.

Chapter 4. MAIN MEASURES FOR COUNTERACTING ILLEGAL ACTIVITY IN THE INFORMATION SPACE

Article 10. Main Measures for Counteracting Illegal Activity in the Information space

To counteract illegal activity in the information space, the States Parties shall:

1) strive to criminalize the use of information resources and/or the manipulation of them in the information space for unlawful purposes, which include the unauthorized dissemination of information, breaches of confidentiality, and damaging the integrity or accessibility of information, and also take legislative or other steps to stipulate the responsibility and hold responsible persons for perpetrating, attempting, being accomplices in or instigating criminalized and socially dangerous actions in the information space;

2) take legislative or other steps to ensure that offenders in the information space receive effective, proportional, and convincing punishment.

Article 11. Measures on Organizing Criminal Procedures

To organize criminal procedures, the States Parties shall:

1) take legislative or other steps to stipulate powers and procedures for the purposes of conducting individual criminal investigations or court trials in cases of the perpetration of criminalized and socially dangerous actions in the information space;

2) ensure the stipulation, execution, and application of powers and procedures for the purposes of conducting individual criminal investigations or court trials in cases of the perpetration of criminalized and socially dangerous actions in the information space in compliance with the provisions and guarantees provided for by the legislation of the State and ensuring the appropriate level of the protection of human rights and freedoms, as well as with the principle of proportionality.

3) take legislative or other steps enabling the law enforcement authorities of the State to take swift action for the protection of certain data, including data on information flows stored in the information and communication infrastructure, when there are reasons to believe that these data are especially vulnerable to loss or manipulation;

4) take legislative or other steps to guarantee timely access of the law enforcement authorities of the State or a person appointed by these authorities to sufficient amounts of data on information flows as to identify service providers and the route of a specific message in its information space;

5) take legislative or other steps which may be necessary to empower the law enforcement authorities of the State to search or gain similar access to information and communication systems and their parts and the data stored therein, as well as to storage media which may contain the data in question, in its territory, and to other data and information and communication systems of their information space which are reasonably implicated in storing the data in question;

6) take legislative or other steps which may be necessary to empower the law enforcement authorities of the State to demand from a person present in its territory and possessing information on the functioning of the relevant information and communication system, its means of protection and the data stored therein, the release of this information, which would allow these authorities to take action, within the scope of their authority, for the purpose of carrying out individual criminal investigations or court trials in cases of the perpetration of criminalized and socially dangerous actions in the information space;

7) take legislative or other steps which may be necessary to empower the law enforcement authorities of the State to collect or record information by means of technology in its territory as well as to demand similar action from service

providers carried out continuously and in cooperation with the law enforcement authorities of the States;

8) take legislative or other steps to establish its jurisdiction over any criminalized and socially dangerous action in the information space perpetrated in the territory of the State, on board a vessel flying the flag of that State, and on board a plane or any other aircraft registered under the laws of that State.

If jurisdiction over an alleged offence is claimed by more than one State Party, the interested parties hold consultations to decide on the most suitable jurisdiction for prosecution.

Chapter 5. INTERNATIONAL COOPERATION IN THE SPHERE OF INTERNATIONAL INFORMATION SECURITY

Article 12. Cooperation between the States Parties

1) The States Parties shall cooperate with each other according to the provisions of this Convention and through other international agreements.

2) The States Parties shall, on the basis of voluntariness and reciprocity, exchange best practices on the prevention, legal investigation, and the liquidation of consequences of crimes, including those related to terrorism, involving the information space. The State Party has the right to request that the information it provides be kept confidential. The State Party that receives such information has the right to refer to it when discussing issues of mutual assistance with the State that provided it.

Article 13. Confidence-Building Measures in the Sphere of the Military Use of the Information space

Each State Party must strive to promote confidence-building measures in the sphere of the military use of the information space, which include:

1) the exchange of national security concepts in the information space;

2) timely exchange of information on crises and threats in the information space and on the steps taken to deal with them;

3) consultations on activities in the information space which may raise concerns of States Parties and cooperation on resolving conflicts of military nature.

Article 14. Consultative Assistance

The States Parties shall cooperate with and consult each other on any issues related to the goals or the implementation of the provisions of this Convention.

CLOSING PROVISIONS

Article 15. Signing of the Convention

This Convention shall be open for signature by all States.

Article 16. Ratification of the Convention

This Convention is subject to ratification. Instruments of ratification shall be deposited with the Secretary-General of the United Nations.

Article 17. Accession to the Convention

This Convention shall remain open for accession by any State. The instruments of accession shall deposited with the Secretary-General of the United Nations.

Article 18. Entering into Force

1) This Convention shall enter into force on the thirtieth day following the date of deposit of the twentieth instrument of ratification or accession with the Secretary-General of the United Nations.

2) For each State ratifying or acceding to this Convention after the deposit of the twentieth instrument of ratification or accession, this Convention shall enter into force on the thirtieth day after the deposit of the instrument of ratification or accession by such State.

Article 19. Amending the Convention

1) Any State Party may propose an amendment and present it to the Secretary-General of the United Nations. The Secretary-General then forwards the proposed amendment to the States Parties requesting them to specify whether they are in favor of holding a conference of States Parties to consider and vote on the proposals. If, within four months of the date of this communication, at least one-third of the States Parties speak in favor of such a conference, the Secretary-General holds this conference under the auspices of the United Nations. Any amendment passed by the majority of the States Parties represented at the

conference and taking part in the vote shall be submitted for approval by the General Assembly.

2) An amendment passed in accordance with paragraph 1 of this article shall enter into force after it is approved by the General Assembly of the United Nations and passed by a two-thirds majority of the States Parties.

3) When the amendment enters into force, it becomes binding for the States Parties that passed it, while the other States Parties remain bound by the provisions of this Convention and any previous amendments passed by these States.

Article 20. Reservations to the Convention

1) The Secretary-General of the United Nations receives and forwards to all parties the texts of reservations made by the States at the time of their ratification or accession.

2) A reservation that is incompatible with the goals and objectives of the Convention is not permitted.

3) Reservations may be withdrawn at any time by notification to the Secretary-General of the United Nations, who then notifies the other States. This notification enters into force on the date on which it is received by the Secretary-General of the United Nations.

Article 21. Denunciation of the Convention

Any State Party may denounce this Convention by written notification to the Secretary-General of the United Nations. The denunciation shall take effect one year following the date on which the notification is received by the Secretary-General.

Article 22. Depositary of the Convention

The Secretary-General of the United Nations shall be appointed as the depositary of this Convention.

Article 23. The original of this Convention, of which the Arabic, Chinese, English, French, Russian and Spanish texts are equally authentic, shall be deposited with the Secretary-General of the United Nations.

IN WITNESS WHEREOF, the undersigned, being duly authorized thereto by their respective Governments, have signed this Convention.