Agreement
on Cooperation in Ensuring International Information Security between the Member States of the Shanghai Cooperation Organization

The Member States of the Shanghai Cooperation Organization (hereinafter referred to as "the Parties")

Noting the significant progress in the development and introduction of new information and communication technologies and tools that are shaping the global information space,

Expressing concern about the threats related to the use of such technology and tools for the purposes inconsistent with the objectives of maintaining international security and stability, both in the civilian and military fields,

Attaching great importance to international information security as one of the key elements of the international security system,

Being convinced that further deepening of trust and development of cooperation between the Parties in ensuring international information security is imperative and in their interest,

Taking into account the important role of information security in ensuring the fundamental human and civil rights and freedoms,

Taking into account the UN General Assembly resolution "Developments in the field of information and telecommunications in the context of international security",

Seeking to limit the threats to international information security, to ensure information security interests of the Parties, and establish an international information environment characterized by peace, cooperation and harmony,

Desiring to create a legal and organizational basis for cooperation between the Parties in the field of international information security,

Have agreed as follows:

Article 1

Basic Terms

For the purposes of interaction between the Parties in the implementation of this Agreement, the basic terms shall be used that are listed in Annex 1 ("List of basic terms in the field of international information security") which shall be an integral part of this Agreement.

Annex 1 may be supplemented, specified, and updated, as appropriate, by agreement of the Parties.

Article 2

Major Threats in the Field of International Information Security

In the course of cooperation under this Agreement, the Parties proceed from the presence of the following key threats to international information security:

1) Developing and using information weapons, preparing and conducting information warfare;

2) Information terrorism;

3) Cybercrime;

4) Use of a dominant position in the information space to the detriment of the interests and security of other States;

5) Dissemination of information prejudicial to the socio-political and socio-economic systems, spiritual, moral and cultural environment of other States;

6) Threats to secure and stable functioning of global and national information infrastructures that are natural and/or manmade.

The agreed understanding by the Parties of the substance of the basic threats listed in this Article is presented in Annex 2 ("List of basic types, sources and features of threats to international information security") which shall be an integral part of this Agreement.

Appendix 2 may be supplemented, specified, and updated, as appropriate, by agreement of the Parties.

Article 3

Major Areas of Cooperation

In view of the threats referred to in Article 2 of this Agreement, the Parties, their authorized representatives, as well as the competent authorities of the Parties defined in accordance with Article 5 of this Agreement, shall cooperate in ensuring international information security in the following major areas:

1) defining, coordinating and implementing necessary joint measures in the field of ensuring international information security;

2) creating of a system of joint monitoring and response to emerging threats in this area;

3) elaborating joint measures for the development of the provisions of the international law limiting the spread and use of information weapons threatening defense capacity, national security and public safety;

4) countering threats related to the use of information and communication technologies for terrorist purposes;

5) combating cybercrime;

6) conducting expertise, research and evaluation in the field of information security necessary for the purposes of this Agreement;

7) promoting secure, stable operation and governance internationalization of the global Internet network;

8) ensuring information security of the critically significant structures of the Parties;

9) developing and implementing joint measures of trust conducive to ensuring international information security;

10) developing and implementing coherent policies and organizational and technical procedures for the implementation of digital signature and data protection in the cross-border exchange of information;

11) exchanging information on the legislation of the Parties on issues of information security;

12) improving the international legal framework and practical mechanisms of

cooperation of the Parties in ensuring international information security;

13) creating conditions for cooperation between the competent authorities of the Parties in order to implement this Agreement;

14) interacting within international organizations and fora on issues of international information security;

15) exchanging experience, training of specialists, holding working meetings, conferences, seminars and other forums of authorized representatives and experts of the Parties in the field of information security;

16) exchanging information on issues related to the cooperation in the basic areas listed in this Article.

By mutual agreement, the Parties or the competent authorities of the Parties may determine other areas of cooperation.

Article 4
Basic Principles of Cooperation

1. The Parties shall cooperate and their activities in the international information space in the framework of this Agreement shall be carried out in such a way that these activities contribute to social and economic development and are compatible with objectives of maintaining international security and stability, consistent with universally recognized principles and norms of the international law, including the principles of peaceful settlement disputes and conflicts, non-use of force, non-interference in internal affairs, respect for human rights and fundamental freedoms, as well as the principles of regional cooperation and non-interference in the information resources of the Parties.

2. The activities of the Parties under this Agreement shall be consistent with the right of each Party to seek, receive and disseminate information, bearing in mind that this right may be restricted by law in order to protect the interests of national security and public safety.

3. Each Party shall have an equal right to protect information resources and critically important structures of its state against misuse and unauthorized

intervention including information attacks on them.

Each Party shall not carry out such actions in respect to the other Party and assist other Parties in the realization of the above right.

Article 5

Main Formats and Mechanisms of Cooperation

1. Within sixty days from the date of entry of this Agreement into force, the Parties, through the Depositary, shall exchange information about the competent authorities of the Parties responsible for the implementation of this Agreement, and the channels of direct exchange of information on specific areas of cooperation.

2. For the purpose of reviewing the implementation of this Agreement, exchange of information, analysis and joint assessment of emerging threats to information security, as well as identification, reconciliation and coordination of joint responses to these threats, the Parties on a regular basis shall hold consultations of the authorized representatives of the Parties and competent authorities of the Parties (hereinafter - the “consultations”).

Regular consultations shall be held by agreement between the Parties, as a rule, once every six months in the Secretariat of the Shanghai Cooperation Organization, or in the territory of one of the Parties at its invitation.

Any Party may initiate early consultations by, offering time and place, as well as the agenda to be subsequently agreed by all the Parties and the Secretariat of the Shanghai Cooperation Organization.

3. Practical collaboration in specific areas of cooperation envisaged by this Agreement may be carried out by the Parties through the competent authorities of the Parties responsible for the implementation of the Agreement.

4. In order to create the legal and institutional framework for cooperation in specific areas, the competent authorities of the Parties may conclude appropriate interdepartmental agreements.

Article 6

Protection of Information

1. This Agreement shall not mandate the Parties to provide information in the framework of the cooperation under this Agreement and it shall not warrant transmitting information in the framework of this cooperation, if the disclosure of such information may harm national interests.

2. In the framework of cooperation under this Agreement, the Parties shall not exchange information regarded as a state secret according to the law of any of the Party. The procedure for the transferring and handling such information, which in specific cases may be considered necessary for the purposes of this Agreement, shall be based on the relevant agreements between the Parties and on the terms thereof.

3. The Parties shall ensure adequate protection of the information transmitted or generated in the course of cooperation under this Agreement provided that this information is not considered as state secret by the laws of any of the Parties, access and dissemination of which is limited in accordance with the law and/or the relevant regulations of any of the Party.

Such information shall be protected in accordance with the legislation and/or the relevant regulations of the receiving Party. Such information shall not be disclosed or transferred without the written consent of the Party that originated this information.

Such information shall be duly marked in accordance with the legislation and/or the relevant regulations of the Parties.

Article 7

Funding

1. The Parties shall bear their own costs of participation of their representatives and experts in the relevant events in support of the implementation of this Agreement.

2. In respect of other costs associated with the execution of this Agreement, in

each case the Parties may agree on a different procedure for funding pursuant to the legislation of the Parties.

Article 8

Relationship with Other International Treaties

This Agreement shall not interfere with the rights and obligations of each of the Parties under other international treaties they are parties to.

Article 9

Dispute Resolution

Disputes over interpretation and application of this Agreement shall be resolved through consultation and negotiations of the Parties.

Article 10

Working Languages

In the framework of the cooperation under this Agreement, Russian and Chinese shall be the working languages.

Article 11

Depositary

The Secretariat of the Shanghai Cooperation Organization shall be the Depositary of this Agreement.

The original of this Agreement shall be deposited with the Depositary that within fifteen days from the date of its signing will send the certified copies thereof to the Parties.

Article 12

Final Provisions

1. This Agreement is concluded for an indefinite period and it shall enter into force on the thirtieth day after the date of receipt by the Depositary of the fourth

written notification of the completion of their internal procedures necessary for its entry into force. In respect of the Party that have completed internal procedures later, this Agreement shall enter into force on the thirtieth day after the date of the receipt by the Depositary of a respective notice.

2. The Parties may amend this Agreement by issuing separate protocols by mutual consent of the Parties.

3. This Agreement is not directed against any state and organization and after its entry into force it shall be open for accession by any state that shares the goals and principles of this Agreement by submission to the Depositary of an instrument of accession. For the acceding state, the present Agreement shall enter into force in thirty days after the date of the receipt by the Depositary of the last notification of acceptance of the accession by the signatory and acceded states.

4. Each Party may withdraw from this Agreement by sending to the Depositary a written a notice at least ninety days prior to the intended date of withdrawal. The Depositary shall notify the other Parties of such intention within thirty days from the date of receipt of such notice.

5. In the event of the termination of this Agreement, the Parties shall take measures to fully meet the commitments in respect of the protection of information, as well as complete previously agreed joint work, projects and other activities carried out in the framework of the Agreement and uncompleted by the time of the Agreement termination.

Done at the city of Ekaterinburg, on June 16, 2009, in a single original, in the Russian and Chinese languages, both texts being equally authentic.

signatures

ANNEX 1

to the Agreement on
Cooperation in the Field of Ensuring
International Information Security
among the Member States of the
Shanghai Cooperation Organization

List of Basic Terms in the Field of International Information Security

"Information Security" means the status of individuals, society and the state and their interests when they are protected from threats, destructive and other negative impacts in the information space;

"Information war" means a confrontation between two or more states in the information space with the aim of damaging information systems, processes and resources, critically important and other structures, undermining political, economic and social systems, psychologically manipulating masses of the population to destabilize society and the State, and also forcing the state to take decisions in the interest of the opposing party;

"Information Infrastructure" means a range of technical tools and systems for formation, generation, transformation, transmission, use and storage of information;

"Information weapons" means information technologies, tools and methods used for the purpose of information warfare;

"Cybercrime" means using information resources and/or influencing them in the information space for illegal purposes;

"Information Space" means a field of activities related to the formation, generation, transformation, transmission, use, storage of information that have an impact, among other things on individual and social consciousness, information infrastructure and information itself;

"Information Resources" means information infrastructure, as well as information itself and its flows;

"Information terrorism" means using information resources in the information

space and/or influencing on them for terrorist purposes;

"Critically important structures" means facilities, systems and institutions of the state, the impact on which may have consequences directly affecting national security, including the security of an individual, society and the state;

"International information security" means the state of international relations that excludes undermining global stability and endangering the security of nations and the world community in the information space;

"Misuse of information resources" means using information resources without appropriate rights or in violation of the established rules, the laws of the Parties or the norms of the international law;

"Unwarranted interference with the information resources" means undue influence on the processes of formation, generation, processing, transformation, transmission, use, storage information;

"Information security threat" means factors hazardous for the individual, society, the state and their interests in the information space.

ANNEX 2

to the Agreement on
Cooperation in Ensuring
International Information Security
between the Member States of the
Shanghai Cooperation Organization

List of Basic Types, Sources, and Features of Threats in the Field of International Information Security

1. Development and application of information weapons, preparation and conduct of information warfare.

The source of this threat is the creation and development of information weapons posing a direct threat to critically important structures of states that may lead to a new arms race and is the main threat in the field of international information security.

Its features include using information weapons for the purpose of preparing and conduction information warfare, as well as of affecting the systems of transportation, communications, and command of air, ballistic missile and other types of defense facilities resulting in a state losing the ability to defend itself in the face of the aggressor and failing to use its legitimate right of self-defense; disrupting the functioning of the information infrastructure facilities resulting in paralyzed governance and decision-making systems of states; destructively impacting critically important structures.

2. Information terrorism.

The source of this threat lies with terrorist organizations and persons involved in terrorist activities, carrying out illegal actions by or in respect of information resources.

Its features include using information networks by terrorist organizations to carry out terrorist activities and bring new supporters into their ranks; destructively impacting information resources leading to a breach of public order; controlling or

blocking media channels; using the Internet or other information networks for terrorist propaganda, creating an atmosphere of fear and panic in the society, as well as negatively impacting information resources in other ways.

3. Cybercrime.

This threat is caused by individuals or organizations engaged in the illegal use of information resources or unwarranted interference with such resources for criminal purposes.

Its features include entering into information systems for compromising the integrity, availability and confidentiality of information; intentionally producing and distributing computer viruses and other malicious programs; implementing DOS-attacks (denial of Service) and other negative impacts; damaging information resources; violating legal rights and freedoms of citizens in the field of information, including intellectual property rights and privacy; using information resources and methods to commit crimes such as fraud, embezzlement, extortion, smuggling, drug trafficking, child pornography, etc.

4. Using dominant position in the information space to the detriment of the interests and security of other countries.

This threat is caused by the unevenness in the development of information technologies in different countries and the current trend of the increased "digital gap" between developed and developing countries. Some states that have advanced in the development of information technologies deliberately hinder the development of other countries and their access to information technologies creating serious danger for countries with insufficient information capacity.

Its features include monopolizing the production of software and hardware for the information infrastructure, limiting the participation of States in international information technology cooperation impeding their development and increasing their dependence of these countries from more developed countries; embedding hidden features and functions in software and equipment supplied to other countries to monitor and influence the information resources and/or critically important structures of these countries; controlling and monopolizing the market of

information technologies and products to the detriment of the interests and security of the states.

5. Dissemination of information harmful to the socio-political and socio-economic systems, spiritual, moral and cultural environment of other States.

This threat is caused by states, organizations, group of persons or particular persons using the information infrastructure for the dissemination of the information harmful to the socio-political and socio-economic systems, spiritual, moral and cultural environment of other States.

It is manifested by the appearance and reproduction in electronic (radio and television) and other media, the Internet and other networks of information exchange of information:

distorting the picture of the political and social system of a state, its foreign and domestic policy, important political and social processes in the country, spiritual, moral and cultural values of its population;

promoting the ideas of terrorism, separatism and extremism;

inciting inter-ethnic, inter-racial and inter-religious strife.

6. Threats to secure and stable functioning of global and national information infrastructures that are natural and/or manmade.

The sources of these threats are natural disasters and other natural hazards and man-made disasters that occur suddenly or as the result of a long process that can have a large-scale devastating impact on the information resources of the state.

They are manifested by the malfunctions of the information infrastructure as a result, destabilization of critical structures, public management and decision-making systems resulting in a direct impact on the security of the state and society.