ty and possible cooperative measures to address them, as well as the concepts referred to in paragraph 2 above, and to submit a report on the results of this study to the General Assembly at its sixty-fifth session;

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

61st plenary meeting
2 December 2008

AGREEMENT
between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security

Unofficial translation

The Governments of the Member States of the Shanghai Cooperation Organization hereinafter referred to as the Parties,

Noting considerable progress in the development and introduction of new information and communication technologies and means shaping the global information space,

Expressing concern about the threats posed by possible use of such technologies and means for the purposes incompatible with ensuring international security and stability in both civil and military spheres,

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

Convinced that further enhancement of confidence and strengthening of interaction between the Parties in the field of ensuring international information security are urgently needed and serve the interests of the Parties,

Considering the important role of information security in the field of ensuring human and civil rights and fundamental freedoms,

Considering the resolutions of the UN General Assembly "Developments in the field of information and telecommunications in the context of international security",

Striving to curb international information security threats, ensure the information security interests of the Parties and create an international information environment of peace, cooperation and harmony,

Wishing to establish a legal and organizational framework for cooperation between the Parties in the field of ensuring international information security,

Have agreed as follows:

Article 1

General Terms

For the purpose of interaction between the Parties in the implementation of this Agreement, the basic terms shall be used which are listed in Annex 1 (List of Basic Terms in the Field of International Information Security) that is an integral part of this Agreement.

Annex 1 may, as necessary, be supplemented, amended and updated as agreed by the Parties.

Article 2

Main Threats in the Field of Ensuring International Information Security

In the process of cooperation in accordance with this Agreement the Parties shall proceed from the assumption that there are the following main threats in the field of ensuring international information security:

1) Development and use of information weapons, preparation for and waging information war;

2) Information terrorism;

3) Information crime;

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

5) Dissemination of information harmful to social and political, social and economic systems, as well as spiritual, moral and cultural spheres of other States;

6) Natural and/or man-made threats to safe and stable operation of global and national information infrastructures.

The agreed understanding by the Parties of the essence of major threats listed in this Article is provided in Annex 2 (List of Major International Information Security Threats, their Sources and Attributes) that is an integral part of this Agreement.

Annex 2 may, as necessary, be supplemented, amended and

updated as agreed by the Parties.

Article 3

Main Areas of Cooperation

Taking into account the threats under Article 2 of this Agreement, the Parties, their authorized representatives and competent authorities of the States of the Parties that are specified under Article 5 of this Agreement shall cooperate in ensuring international information security in the following main areas:

1) identifying, agreeing and implementing necessary collective measures in the field of ensuring international information security;

2) establishing a system to monitor and jointly respond to threats emerging in this area;

3) elaborating collective measures regarding development of norms of international law to curb proliferation and use of information weapons that endangers the defensive capability, national and public security;

4) countering threats of using ICTs for terrorist purposes;

5) countering information crime;

6) conducting examination, research and assessment in the field of ensuring information security that is necessary for the purposes of this Agreement;

7) assisting secure and stable functioning and internationalization of global Internet governance;

8) ensuring information security of critical structures of the States of the Parties;

9) elaborating and implementing joint confidence-building measures to ensure international information security;

10) elaborating and implementing coordinated policies and organizational and technical procedures for using the electronic digital signature and information protection in trans-border information exchange;

11) information exchange on legislation of the States of the Parties on issues of ensuring information security;

12) improving the international legal base and practical mechanisms of cooperation among the Parties in ensuring international information security;

13) creating conditions for interaction among the competent authorities of the States of the Parties in order to implement this Agreement;

14) interacting within the framework of international organizations and forums on ensuring 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) information exchange on issues concerning implementation of cooperation in the main areas listed in this Article.

The Parties or the competent authorities of the States of the Parties may determine other areas of cooperation by mutual agreement.

Article 4

General Principles of Cooperation

1. The Parties shall cooperate and act in the international information space within the framework of this Agreement in such a way that these activities contribute to social and economic development and comply with maintaining international security and stability, generally recognized principles and norms of international law, including the principles of peaceful settlement of disputes and conflicts, non-use of force, non-interference in internal affairs, respect for human rights and fundamental freedoms and the principles of regional cooperation and non-interference in the information resources of the States of the Parties.

2. The activities of the Parties within the framework of this Agreement should be compatible with the right of each Party to search, obtain and disseminate information given that this right can be restricted by law in order to protect national and public security.

3. Each Party shall have equal rights to protect the information resources and critical structures of their States from illicit use and unauthorized interference, including information attacks.

Each Party shall not carry out such actions against another Party and shall assist other Parties in exercising the above-mentioned right.

Article 5

Main Forms and Mechanisms of Cooperation

1. Within 60 days after the date on which this Agreement has entered into force, the Parties shall exchange data, through a depositary, on the competent authorities of the States of the Parties responsible for implementing this Agreement and channels of direct information exchange on specific areas of cooperation.

2. In order to review the implementation of this Agreement, information exchange, analysis and joint assessment of emerging threats to information security, as well as to determine, agree and coordinate joint response measures, the Parties should hold regular consultations between the authorized representatives of the Parties and competent authorities of the

States of the Parties (hereinafter - consultations).

Regular consultations shall be usually held, as agreed by the Parties, once in six months at the Secretariat of the Shanghai Cooperation Organization or in the territory of the State of one of the Parties at its invitation.

Any of the Parties may initiate extraordinary consultations proposing the time, venue and agenda for subsequent approval by all the Parties and the Secretariat of the Shanghai Cooperation Organization.

3. The Parties may engage in practical interaction in specific areas of cooperation provided for by this Agreement through the competent authorities of the States of the Parties responsible for implementing this Agreement.

4. In order to lay the legal and organizational foundation for cooperation in specific areas, the competent authorities of the States of the Parties may conclude appropriate interagency treaties.

Article 6

Protection of Information

1. This Agreement shall not oblige the Parties to provide information within the framework of cooperation in accordance with this Agreement and shall not provide basis for transferring information within the framework of this cooperation if the disclosure of such information might damage national interests.

2. Within the framework of cooperation in accordance with this Agreement, the Parties shall not exchange information that constitutes State secret and/or State secrets by law of the State of any of the Parties. The procedures of transferring and processing such information that may be considered necessary in certain cases for implementation of this Agreement shall be regulated subject to the terms and conditions of relevant treaties signed between the Parties.

3. The Parties shall ensure appropriate protection of the information transferred or generated in the course of cooperation within the framework of this Agreement, that shall not constitute State secret and/or State secrets according to the legislation of any of the States of the Parties, access and dissemination of which are restricted according to the legislation and/or relative regulations of any of the States of the Parties.

Such information shall be protected according to the legislation and/or relevant regulations of the State of the receiving Party. Such information shall not be disclosed or transferred without the written consent of the Party, which is the source of this information.

Such information shall be properly designated in accordance with the legislation and/or relevant regulations of the States of the Parties.

Article 7

Financing

1. The Parties shall independently bear the costs of participation of their representatives and experts in relevant activities relating to the implementation of this Agreement.

2. As for other costs of implementation of this Agreement, the Parties may agree upon other financing procedures in each particular case in accordance with the legislation of the States of the Parties.

Article 8

Relationship to other International Treaties

This Agreement shall not affect the rights and obligations of each of the Parties under other international Treaties to which their States are parties to.

Article 9

Settlement of Disputes

Disputes that may arise out of interpretation or application of the provisions of this Agreement shall be settled through consultations and negotiations.

Article 10

Working Languages

The working languages for cooperation under this Agreement shall be Russian and Chinese.

Article 11

Depositary

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

The original copy of this Agreement shall be deposited with the Depositary that shall, within fifteen days following the date of its signature, send its certified copies to the Parties.

Article 12

Final Provisions

1. This Agreement shall be concluded for an indefinite period of time and enter into force on the thirtieth day following the date of receiving by the Depositary of the fourth written notification on the completion by the Parties of respective internal procedures necessary for its entry into force. For the Party that has completed its domestic procedures afterwards, this Agreement shall come into force on the thirtieth day from the date of receiving by the Depositary of the appropriate notification.

2. The Parties may amend this Agreement, which shall be formalized by mutual consent of the Parties, in a separate protocol.

3. This Agreement is not directed against any other States or organizations and upon its entering into force shall be open for accession by any State that shares the goals and principles of this Agreement, by depositing of the document of accession with the Depositary. For the acceding State, the present Agreement shall come into force on the thirtieth day following the date of receiving by the Depositary of the last notification of consent to such accession of both the signatory and acceding States.

4. Each Party can withdraw from this Agreement, by sending to the Depositary a written notification of its intention no less than ninety days before the expected date of withdrawal. The Depositary shall inform other Parties of this intention within thirty days from the date of receipt of such notification.

5. In case of termination of this Agreement the Parties shall undertake measures to fulfill their obligations on information security completely, as well as earlier agreed joint efforts, projects and other measures carried out under this Agreement and that have not been accomplished by the moment of the termination of this Agreement.

Done at Yekaterinburg on 16 June 2009 in a single original copy in Russian and Chinese, both texts being equally authentic.

For the Government
of the Republic of Kazakhstan

For the Government
of the People's Republic of China

For the Government
of the Kyrgyz Republic

For the Government
of the Russian Federation

For the Government
of the Republic of Tajikistan

For the Government
of the Republic of Uzbekistan

ANNEX 1
to the Agreement between the Governments
of the Member States of the Shanghai
Cooperation Organization on Cooperation
in the Field of International Information Security

LIST

of basic terms in the field of international information security

"Information security" - security of the individual, society, state and their interest from threats, destructive and other negative impacts in the information space;

"Information war" - confrontation between two or more states in the information space aimed at damaging information systems, processes and resources, critical and other structures, undermining political, economic and social systems, mass psychologic brainwashing to destabilize society and state, as well as to force the state to taking decisions in the interest of an opposing party;

"Information infrastructure" - array of technical means and systems to generate, transform, transfer, use and store information;

"Information weapon" - information technologies, ways and means of waging an information war;

"Information crime" - use of and/or attack on information resources in the information space for illegal purposes;

"Information space" - field of activities related to generating, transforming, transferring, using and storing information which influences, in particular, individual and public mind, information infrastructure and information as such;

"Information resources" - information infrastructure, as well as information as such and its flows;

"Information terrorism" - use of and/or attack on information resources in the information space for terrorist purposes;

"Critical structures" - public facilities, systems and institutions attacks on which may cause consequences directly affecting national security, including that of the individual, society and state;

"International information security" - international relations environment which rules out violating world stability

and threatening the security of states and world community in the information space;

"Unlawful use of information resources" - use of information resources without relevant rights or in violation of the existing rules and laws of states or norms of international law;

"Unauthorized interference with the information resources " - unlawful impact on the processes of generating, processing, transforming, transferring, using and storing information;

"Information security threat" - factors which pose a threat to the individual, society, state and their interest in the information space.

ANNEX 2
to the Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security

LIST

of Major International Information Security Threats, their Sources and Attributes

1. Development and use of information weapons, preparing and waging information war.

This threat emanates from creating and developing information weapons that pose an immediate danger to critical structures of States which might lead to a new arms race and represents a major threat in the field of international information security.

Among its characteristics are the use of information weapons to prepare and wage information war, and impact transportation, communication and air control systems, missile defense and other types of defense facilities, as a result of which the State looses its defense capabilities in the face of aggressor and fails to exercise its legitimate

right to self-defense; breaching information infrastructure operation, which leads to the collapse of administrative and decision-making systems in the States; and destructive impact on critical structures.

2. Information terrorism.

This threat emanates from terrorist organizations and individuals involved in terrorist activities acting unlawfully through information resources against regarding them.

It is characterized by the use of information networks by terrorist organizations to carry out terrorist activities and recruit new supporters; destructive impact on information resources leading to disruption of public order; control or blocking of mass media channels; use of the Internet or other information networks for terrorist propaganda, creating an atmosphere of fear and panic in the society, as well as other negative impacts on the information resources.

3. Information crime.

The sources of this threat include individuals or organizations involved in the unlawful use of information resources or unauthorized interference in such resources for criminal purposes.

It is characterized by breaching information systems to compromise information integrity, accessibility and confidentiality; deliberate production and dissemination of computer viruses and other malicious programs; DoS-attacks (denial of service) and other negative impacts; damage to information resources; violation of legitimate rights and freedoms of citizens in the information sphere, including intellectual property and privacy; use of information resources and methods in order to commit such crimes as fraud, theft, extortion, smuggling, illicit drug trafficking, distribution of child pornography, etc..

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

The sources of this threat include the uneven development of information technologies in various states and the existing trend to increase the "digital gap" between the developed and developing countries. A number of states that have advantages in the development of information technologies deliberately constrain the development of other countries and access to information technologies, which

creates a serious danger for the states with insufficient information potential.

It is characterized by monopolization of production of software and hardware of information infrastructures, limitation of state participation in international information technology cooperation which hampers their development and increases the dependence of these countries from the more developed states; embedding of hidden options and functions into the software and hardware supplied to other countries in order to control and influence information resources and/or critical structures of these countries; control and monopolization of 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 emanates from states, organizations, groups of people or individuals that use the information infrastructure to disseminate information harmful to the socio-political and socio-economic systems, spiritual, moral and cultural environment of other States.

It is characterized by the appearance and replication of information in digital (radio and television) and other mass media, on the Internet and other information exchange networks that:

distorts the perception of the political system, social order, domestic and foreign policy, important political and social processes in the State, spiritual, moral and cultural values of its population;

promotes the ideas of terrorism, separatism and extremism;

stirs up inter-ethnic, interracial and inter-confessional hostility.

6. Natural and/or man-made threats to safe and stable operation of global and national information infrastructures.

These threats emanate from natural disasters and other dangerous natural phenomena, as well as man-made disasters that occur suddenly or as a result of a long process that can cause large-scale impact on the information resources of the State.

They are characterized by disruption of operation of information infrastructure facilities and, as a consequence, destabilization of critical structures, state management and decision-making systems, which directly affects state and social security.