GOVERNMENT OF THE RUSSIAN FEDERATION

ORDER

on April 30, 2015 No 788-p
MOSCOW

**On signing the Agreement between the Government of the Russian Federation
and the Government of the People's Republic of China
on cooperation in ensuring international
information security**

In accordance with paragraph 1 of Article 11 of the Federal Law "On international treaties of the Russian Federation," Russian Foreign Ministry submitted to approve with other interested federal bodies of executive power and pre-crafted with the Chinese side a draft agreement between the Government of the Russian Federation and the Government of the People's Republic of China on cooperation in the field of International Information Security (attached).
Instruct the Russian Foreign Ministry to hold talks with the Chinese side and on reaching an agreement to sign on behalf of the Government of the Russian Federation said Agreement, allowing to make the annexed draft changes without principle.

Prime Minister
The Russian Federation D. Medvedev

Agreement
between the Government of the Russian Federation
and the Government of the People's Republic of China
on cooperation in ensuring international
information security

The Government of the Russian Federation and the Government of the People's Republic of China, hereinafter referred to as the Parties,
Guided by the provisions of the Treaty of Good-Neighborliness, Friendship and Cooperation between the Russian Federation and the People's Republic of China on July 16, 2001,
Noting the significant progress in the development and implementation of new information and communication technologies that shape the global information space,
Attaching great importance to the role of ICT in promoting social and economic development for the benefit of humanity and the maintenance of international peace, security and stability,
Expressing concern about threats related to the use of such technology in the civilian and military purposes inconsistent with the objectives of international peace, security and stability, in order to undermine the sovereignty and security of states and interference in their internal affairs and infringement of the privacy of citizens, destabilize the political and socio-economic situation, inciting ethnic and religious hatred,
Attaching great importance to international information security as one of the key elements of the international security system,
Reaffirming that the sovereignty and international norms and principles derived from the state sovereignty, apply to the conduct of States in the framework of activities related to the use of information and communication technologies, and the jurisdiction of States over information

infrastructure in their territory, and that the state has the sovereign right to define and implement public policies on matters relating to information and telecommunications network "Internet", including security,
emphasizing the joint work within the framework of the Shanghai Cooperation Organization,
Convinced that the further deepening of trust and development of cooperation between the Parties in the field of information and communication technologies are imperative, and in their interest,
Taking into account the important role of information security to ensure the fundamental rights and freedoms of man and citizen,
Attaching great importance to the balance between security and human rights in the field of information and communication technologies,
In order to prevent threats to international information security, information security to ensure the interests of the Parties in order to create an international information environment, which is characterized by peace and cooperation,
Trying to form a multilateral, transparent and democratic international system of control of information and telecommunications network "Internet" in order to control the internationalization of information and telecommunications network "Internet" and equal rights of states to participate in this process, including the democratic governance of the main resources of information and telecommunications network "Internet "and their equitable distribution,
Desiring to create a legal and institutional framework for cooperation of the Parties in the field of international information security,
Have agreed as follows:

Article 1
Basic concepts

For the purposes of interaction between the Parties in the implementation of this Agreement, the basic concepts, the list of which is given in annex, which is an integral part of this Agreement. The said application may be supplemented, as necessary, refined and updated by agreement of the Parties.

Article 2
The main threats in the field of international information security

In the implementation of cooperation under this Agreement The Parties believe that the main threats to international information security are the use of information and communication technologies:
1) to carry out acts of aggression aimed at the violation of the sovereignty, security, territorial integrity of States and a threat to international peace, security and strategic stability;
2) for the application of economic and other damage, including through the provision of a destructive impact on the objects of the information infrastructure;
3) for terrorist purposes, including for the promotion of terrorism and involvement in terrorist activities and more supporters;

4) to commit offenses and crimes, including those related to unauthorized access to computer data;
5) to interfere in the internal affairs of States, violations of public order, incitement of ethnic, racial and religious hatred, propaganda of racist and xenophobic ideas and theories that give rise to hatred and discrimination, incitement to violence and instability, as well as to destabilize the internal political and socio-economic situation , violation of government;
6) for the dissemination of information harmful to the socio-political and socio-economic systems, spiritual, moral and cultural environment of other States.

Article 3
Key areas of cooperation

1. In view of the major threats referred to in Article 2 of this Agreement, the Parties authorized representatives and the competent authorities of the Parties, which are determined in accordance with Article 5 of this Agreement, shall cooperate in ensuring international information security in the following areas:
1) definition, coordination and implementation of the necessary cooperation in ensuring international information security;
2) establishment of channels of communication and contacts with a view to jointly respond to threats in the sphere of international information security;
3) cooperation in the development and promotion of international law in order to ensure national and international information security;
4) joint response to the threats in the field of international information security as defined in Article 2 of this Agreement;
5) the exchange of information and cooperation in law enforcement to investigate cases involving the use of information and communication technologies for terrorist and criminal purposes;
6) the development and implementation of the necessary joint confidence-building measures that contribute to ensuring international information security;
7) cooperation between the competent authorities of the Parties to ensure the safety of the critical information infrastructure of the Parties, technology exchange and cooperation between the competent authorities of the Parties in the field of Computer Emergency Response;
8) the exchange of information on the legislation of the Parties on issues of information security;
9) to contribute to improving the international legal framework and practical mechanisms of cooperation of the Parties in ensuring international information security;
10) the creation of conditions for cooperation between the competent authorities of the Parties in order to implement this Agreement;
11) to enhance cooperation and coordination among States Parties on issues of international information security within the framework of international organizations and fora (including the United Nations, the International

Telecommunication Union, the International Organization for Standardization, the Shanghai Cooperation Organization, the BRICS countries, the Regional Forum of the Association of South-East Asian security and others);
12) the promotion of research in the field of international information security, joint research work;
13) joint training of specialists, exchange of students and teachers from specialized higher education institutions;
14) conduct of meetings, conferences, seminars and other forums delegates and experts of the Parties in the field of international information security;
15) the establishment of a mechanism for cooperation between the competent authorities of the Parties for the exchange of information and sharing of information on existing and potential risks, threats and vulnerabilities in the area of information security, their identification, assessment, research, mutual information about them and to prevent their occurrence.
2. The Parties or the competent authorities of the Parties may, by mutual agreement to define other areas of cooperation.

Article 4
General principles of cooperation

1. The Parties shall cooperate in the field of ensuring international information security in the framework of this Agreement in such a way that such cooperation contributed to social and economic development, it is compatible with the maintenance of international peace, security and stability, and consistent with generally recognized principles and norms of international law, including the principles of peaceful settlement of disputes and conflicts, non-use or threat of force, non-interference in internal affairs, respect for human rights and fundamental freedoms and the principles of bilateral 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 impart information, bearing in mind that such a right can be restricted by the legislation of the Parties in order to ensure national security.
3. Each Party shall have an equal right to protection of information resources of their state against misuse and unauthorized intervention, including by cyber attacks on them.
Each Party shall not with respect to the other Party of such actions and assist the other Party in implementing this law.

Article 5
Basic forms and mechanisms of cooperation

1. Practical cooperation in specific areas of cooperation under this Agreement, the Parties may carry out by the competent authorities of the Parties responsible for the implementation of this Agreement. Within 60 days of the entry into force of this Agreement, the Parties will exchange through diplomatic channels the data

on competent authorities of the Parties responsible for the implementation of this Agreement.
2. In order to create a legal and institutional framework for cooperation in specific areas of the competent authorities of the Parties may enter into appropriate agreements interdepartmental character.
3. Rule of the exchange defined in subparagraph 15 of paragraph 1 of Article 3 of this Agreement, as well as used for this message formats and means of protection of information transmitted are determined by corresponding agreements between the competent authorities of the Parties.
4. In order to review the implementation of this Agreement, exchange information, analysis and joint assessment of emerging threats to information security, as well as the determination to harmonize and coordinate a joint response to such threats Parties shall hold consultations on a regular basis, and authorized representatives of the competent authorities of the Parties. Consultations are carried out by agreement of the Parties, usually 2 times a year, alternately in the Russian Federation and the People's Republic of China. Each of the Parties may initiate additional consultation, offering the time and place of their implementation, as well as the agenda.

Article 6
Data protection

1. The Parties shall provide adequate protection for transferred or created in the course of cooperation under this Agreement, the information to which access is limited and distribution in accordance with the legislation of the Parties. Protection of such information in accordance with the legislation and (or) the relevant regulatory legal acts of the receiving Party. Such information shall not be disclosed, is not transferred without the written consent of the Party, which is the source of this information, and duly designated in accordance with the legislation of the Parties.
2. Protection of State Secrets of the Russian Federation and (or) protection of state secrets of China in the course of cooperation under this Agreement shall be performed in accordance with the Agreement between the Government of the Russian Federation and the Government of the People's Republic on mutual protection and ensure the safety of classified information by May 24, 2000 year, as well as the legislation and (or) the relevant regulatory legal acts of the Parties.

Article 7
Funding

1. The Parties shall bear their own costs of participation of their representatives, and experts in the relevant measures for the implementation of this Agreement.
2. In respect of other costs associated with the execution of this Agreement, the Parties in each case may agree on a procedure for funding in accordance with the legislation of the Parties.

Article 8
Relation to other international agreements

This Agreement shall not affect the rights and obligations of each of the Parties under other international treaties to which it is a member, and not directed against any third country.

Article 9
Settlement of Disputes

The Parties shall resolve disputes that may arise in connection with the interpretation or application of this Agreement through consultations and negotiations between the competent authorities of the Parties and, if necessary, through diplomatic channels.

Article 10
Final Provisions

1. This Agreement is concluded for an indefinite period and shall enter into force on the 30th day following the date of receipt through diplomatic channels of the last written notification on fulfillment by the Parties of internal procedures necessary for its entry into force.
2. The Parties may make changes to this Agreement, which by mutual agreement of the Parties executed a separate protocol.
3. Operation of this Agreement may be terminated at the expiration of 90 days from receipt of one of the Parties through diplomatic channels, written notice to the other Party of its intention to terminate this Agreement.
4. In the event of termination of this Agreement, the Parties shall take measures to fully implement the obligations to protect information and ensure compliance with previously agreed joint activities, projects and other activities carried out under this Agreement and not completed at the time of termination of this Agreement.

Done at … on … 2015 in two copies, in Russian and Chinese languages, both texts being equally authentic.

For the Government of
of the Russian Federation

For the Government
the People's
Republic of China

APPENDIX

To the agreement in the Field of International Information Security between the government of the Russian Federation and the government of the People's Republic of China

List of basic notions used for cooperation purposes of all parties within the context of the implementation of the agreements between the government of the Russian Federation and the government of the People's Republic of China on cooperation in the area of ensuring intentional information security

"Information Security" - describes the practice of defending the information of individuals,society and the government from unauthorized access, use, disclosure, disruption,modification, perusal, inspection, recording or destruction.

"Information infrastructure" - defines the set of technical means and systems of transformation, transmission, use and storage of information.

"Information space"- the sphere of activity related to creation/development, transformation, transmission, use and storage of information with impact on individual and public awareness, information infrastructure and actual information.

"Information resources"- information infrastructure, including information itself, and data flows.

"Information/Data Security"- range of legal, organizational and technical measures to ensure integrity (specialty), confidentiality and accessibility of information

„Subjects of the critical information infrastructure "- IT systems, telecommunication networks of governmental bodies; IT systems, telecommunication networks and automated process control systems operating in the arms industry, public health sector, areas of transportation, communication, financial and monetary sphere, energy, fuel industry, nuclear industry, space industry, mining sector, metallurgical industry and the chemical industry.

"Computer Attack" – a deliberate action through software systems (hardware and software) on the information resources, telecommunication networks and the automated process control systems, being implemented in order to disrupt the running of and (or) to breach security

“Improper use of the information resources”- the use of information systems and resources without the relevant entitlement or in violation of the established rules, legislation of each of the parties, or the norms of international law.

“Unauthorized interference with information resources”- the undue influence on the processesof establishing, using, transmitting, processing and storing information.

“Threat to information security“- factors that endanger the basic interests of the individual, of society and of the state in the information area.