

To the Ministry of Foreign Affairs of the Russian Federation

To the Federal Security Service of the Russian Federation

To the Ministry of Internal Affairs of the Russian Federation

Information Request

In accordance with Articles 38 and 39 of the Law of the Russian Federation "On Mass Media", the editorial board of the "Mediazona" (the certificate of registration as the media EL No. FS77-59216 issued by Roskomnadzor on August 22, 2014) submits the current request for information and documents on international cooperation and sharing surveillance information in the field of combating cybercrime and ensuring information security.

The background

On March 23, while answering questions during a lecture for senior officers of the Military Academy of the General Staff in Moscow Foreign Minister Sergey Lavrov spoke about Russia's participation in the issues of information and cyber security, and also mentioned the proposal put forward by Russia in the UN to develop an international treaty on cybersecurity. In particular he said:

“Question: Recent experience shows that, in terms of the damage they cause, aggressive actions in the media at times have consequences similar to the use of weapons of mass destruction. In your opinion, isn't it time, at the UN, in the format of bilateral ties with other states, to move forward with drafting and signing a comprehensive treaty in this field, similar to strategic arms limitation treaties?

Sergey Lavrov: We've been working on this for several years now. Russia put forward an initiative that became known at the UN as International Information Security [Initiative] <...> Overall, we believe (and we have already submitted this proposal) that it is time to draft an international convention on cyber security, including the elimination of threats and risks related to hacking.“¹

The issues concerning information security and countering threats in this area has been consistently one of the priorities of Russian foreign policy over the past few years.

On November 15, 2005, president Putin instructed the Russian Foreign Ministry to sign on behalf of the Russian Federation CE Convention on Cybercrime. The Convention was never signed, and the president's order was canceled in 2008.

However, in 2011 the Russian Foreign Ministry published the concept of the Convention on Ensuring International Information Security, developed by the Security Council of the Russian Federation, the Ministry of Foreign Affairs

¹ http://www.mid.ru/en/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/2702537

and the Institute for Information Security Problems of Moscow State University, which was subsequently discussed with working groups from India and China.

According to the document, among the main threats to international peace and security in the information space, the developers saw:

- “- 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;
- 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;
- 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”².

In January 2015, the Permanent Representatives of Kazakhstan, China, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations submitted to the General Assembly the revised Code of Conduct for International Information Security, according to which all states that voluntarily comply with the Code pledged:

- “(4) To cooperate in combating criminal and terrorist activities that use information and communications technologies and information and communications networks, and in curbing the dissemination of information that incites terrorism, separatism or extremism or that inflames hatred on ethnic, racial or religious grounds”³“

On May 8, 2015, the Government of the Russian Federation and the Government of the People's Republic of China signed an agreement on cooperation in the field of ensuring international information security⁴, according to which the parties agreed to share information and to cooperate in law enforcement for the purpose of investigating cases involving the use of information and communication technologies for terrorist and criminal purposes (Clause 5, Part 1, Article 3).

On December 5, 2016 President Putin approved the Doctrine of Information Security of the Russian Federation. According to the document, one of the main threats to the country's security is that

- “14. The scale of computer criminality is growing, primarily in the credit and financial sphere, the number of crimes related to the violation of constitutional rights and freedoms, including those

2 http://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptlCk6BZ29/content/id/191666

3 http://www.un.org/ga/search/view_doc.asp?symbol=A/69/723&referer=/english/&Lang=E

4 <http://government.ru/media/files/5AMAccs7mSIXgbfflUa785WwMWcABDJw.pdf>

relating to privacy, personal and family secrets, in the processing of personal data with the use of information technology. However, the methods and means of committing such crimes are becoming more sophisticated.”

Thus, it can be seen that the Russian Federation is making significant efforts to maintain and promote international cooperation, including share of information, in the field of countering cybercrime and ensuring information security. This, in particular, is evidenced by the statement of Minister Lavrov, made on March 23, 2017. At the same time, the refusal of the Russian Federation to sign the Budapest Convention on Cybercrime, in particular, because of disagreement with the provisions of Article 32 on "cross-border access," testifies to the existing concerns about possible access of law enforcement agencies and intelligence services of foreign states to computer information, even from open sources.

Nevertheless, there is practically no information on specific actions taken by Russian law enforcement agencies in this area in open sources.

In this regard we respectfully ask

- 1) To provide us with the information on any bilateral, multilateral, interagency, intergovernmental and/or interstate agreements in the field of combating cybercrime and countering threats in the information space were concluded by the Russian Federation (or its agencies), including documents providing the exchange of surveillance information. If possible, please provide the texts of these agreements in electronic form.
- 2) Within the scope of yours competence, provide answers to the following questions:
 - a. Under what circumstances the Russian Federation may share surveillance data on cybercrime with another country?
 - b. Are there any limitations on the sharing of surveillance data on cybercrime with other countries?
 - c. Under what circumstances the Russian Federation may request surveillance data on cybercrime from foreign states?
 - d. What is the procedure for requesting information from foreign states and providing information at the request of foreign states? Which state agencies of the Russian Federation and foreign states directly interact?
 - e. What specific measures to ensure compliance with the rights and legitimate interests of citizens of the Russian Federation are taken in the course of interaction with foreign countries in this area?

Information on this request is asked to be provided in electronic form by email _____. In case of a complete or partial refusal to provide information, please indicate specific reasons that prevent the provision of information, with

reference to the relevant provisions of the law.

We are aware that sharing information concerning investigative activities is a very sensitive topic that may affect non-public spheres. Nothing in this request should be construed as an attempt to get access to a state secret or other secret protected by law. However, if we are denied on these grounds in providing information on this request, we also ask you to indicate the specific circumstances confirming that the requested information is a state secret.

At the same time, let us remind that while preparing a response to this request, you should be guided by the constitutional principles of freedom of speech and openness of information on the activities of public authorities that require a balance of national security interests and the right of the public to receive information. In particular, this is important when the it is a duty of the press to impart information on all matters of public interest.

Editor in cheif _____ / _____

Date, place