International Journal of Social Science Research and Review

http://ijssrr.com
editor@ijssrr.com
Volume 6, Issue 3
March, 2023
Pages: 475-479

# International Cooperation within the SCO in the Field of Information Security

Sadriddin Akramovich Rakhimov

Doctor of Philosophy (PhD) in Historical Sciences, Journalism and Mass Communications University of Uzbekistan

Email: sadriddin.r@mail.ru

http://dx.doi.org/10.47814/ijssrr.v6i3.1131

## *Abstract*

The article discusses the establishment of multilateral cooperation within the framework of the Shanghai Cooperation Organization in combating threats and challenges in the information sphere. The study also examines the activities of the Regional Anti–Terrorist Structure and other SCO mechanisms to ensure international information security, as well as the practical experience accumulated by the Organization’s member countries in countering the use of the Internet for terrorist purposes.

***Keywords:*** *SCO; RATS; Foreign Policy; Globalization; International Organization; Regional Security; Cooperation*

## *Introduction*

In the conditions of the modern world, against the background of growing tensions in a number of regions and increasing threats to international security, including in the global information space, as well as the increasing influence of globalization processes on ensuring stability, both at the national level and on the scale of the entire Central Asian region, has its dependence on the formation of effective mechanisms of multilateral cooperation.

With the development of man–made civilization and information and communication technologies, the complexity and variety of forms of new security threats that lie in wait for modern societies have become obvious. Transnational phenomena such as terrorism, extremism, drug smuggling and weapons have changed traditional ideas about the stability and security of any single State. In modern conditions, no state in the world is able to fully resist non–traditional security threats alone, even the borders between countries are not an obstacle for them. In such a situation, the Republic of Uzbekistan, being committed to the development of equal and mutually beneficial relations with all interested countries, focuses its main efforts in foreign policy on enhancing bilateral and multilateral cooperation, within the framework of international organizations and institutions, in order to create favorable conditions for the sustainable development of the country, as well as ensuring peace and stability in Central Asia.

*Multilateral cooperation in combating threats and challenges in the information sphere.* In its foreign policy, the Republic of Uzbekistan attaches great importance to the creation of effective mechanisms for practical multilateral cooperation, which include the Shanghai Cooperation Organization (SCO).

Uzbekistan, being a co–founder of the SCO, stands for a consistent and systematic solution to the issues of effective counteraction to new challenges and threats to international security, including in the information and communication network Internet. In particular, speaking about the negative consequences of terrorism for the world community, President of the Republic of Uzbekistan Shavkat Mirziyoyev, in his speech at the Astana SCO Summit (2017), noted that one of the solutions to this issue is giving the SCO Regional Anti–Terrorist Structure the authority to organize a system for monitoring emerging threats in the global information space and countering them [1]. For in the context of unprecedented progress in the development and use of information and communication technologies, which create a global information space and pose a global information threat to the national interests of sovereign States, Information security is a one of the key elements of the international security system.

Moreover, in the context of information globalization, the issues of strengthening multilateral cooperation in combating threats and challenges in the information sphere are becoming topical, because intensive development and introduction of modern information international terrorism also offers new opportunities in the various spheres of human activity. In particular, in modern times, international terrorist organizations (MTOs) use new information technologies (telecommunications, Internet, etc.) predominantly for ensure the functioning and coordination of its structural units and clandestine cells, organize and carry out terrorist acts, to disseminate information on the terrorist act committed by them, attract financial resources, conducting ideological propaganda activities for moral and psychological support of terrorist groups and recruitment of new members.

One of the most dangerous forms of modern terrorism is cyberterrorism. For example, in May 2017, a large–scale cyberattack was carried out using the WannaCry virus, as a result of which, according to experts from the United States, about 300 thousand computers in at least 150 countries were infected, including computer systems of the German railway concern Deutche Bahn, the Spanish telecommunications system Telefonica, Russian Megafon, Russian Railways, the Ministry of Internal Affairs and the Investigative Committee of the Russian Federation [2]. According to Stu Sjouwerman, executive director of the American IT company KnowBe4, the estimated damage caused by WannaCry in just the first four days exceeded $1 billion, given the huge downtime caused by this action by large companies around the world [3]. Due to the weak approach to the analysis and monitoring of the information space in many countries, various destructive forces continue to use the interest of the Internet audience to carry out their hostile actions.

At the same time, it should be noted that the SCO member states have already accumulated some experience of cooperation in the field of information security. Taking into account the importance and relevance of this problem and in order to improve the coordination and interaction of the competent authorities in the field of international information security within the framework of the SCO, the necessary organizational and legal basis has been created and work has been launched to strengthen the interaction of the competent authorities of the Organization countries in the field of identifying, preventing and suppressing the use of international terrorist organizations in their criminal activities of modern information and communication technologies and means.

Thus, in the Agreement signed on June 16, 2009 between the governments of the SCO member states on cooperation in the field of ensuring international information security, the countries of the association, taking into account the presence of possible threats in this area, identified the main areas of multilateral cooperation as the development of joint measures to develop international law in the field of limiting the proliferation and use of information weapons that pose threats to defense capability and national security; countering information crime and threats to the use of information and communication technologies for terrorist purposes; promoting the safe, stable functioning and internationalization of the global Internet network management; ensuring information security of critical facilities of the SCO countries; development and implementation of an agreed policy and organizational and technical procedures to ensure international information security and the implementation of information protection in cross–border information exchange; cooperation within the framework of international organizations and forums in matters of ensuring international information security, training of specialized specialists, as well as in other areas of this sphere [4].

According to this document, the countries of the association carry out cooperation and their activities in the international information space in such a way that such activities contribute to socio–economic development and are compatible with the tasks of maintaining peace and stability, comply with 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 human rights and fundamental freedoms, as well as the principles of regional cooperation and non–interference in the information resources of the participating countries. At the same time, this Agreement is not a basis for the transfer of data within the framework of this cooperation, the disclosure of which may pose a threat to national interests.

*The role of the Regional Anti–Terrorist Structure in countering the use of the Internet for terrorist purposes.* International terrorism, which is one of the global problems of our time, requires active consolidation of international efforts.

The SCO Regional Anti–Terrorist Structure (RATS), established in 2004 with headquarters in Tashkent, plays an important role in maintaining and strengthening security in the SCO space, coordinating the practical activities of the competent authorities of the member states in the fight against terrorism and extremism, as well as in developing cooperation with the anti–terrorist structures of international organizations.

During its activity, the RATS have made a significant contribution to the development of the SCO and ensuring regional stability and security.

Within the framework of the Joint Working Group of Experts established in 2013 by the competent authorities of the SCO member States and representatives of the RATS, targeted measures are being taken to prevent and suppress the use or threat of use of computer networks for terrorist purposes, information is being exchanged on significant identified facts of information dissemination in social networks, etc. The next meeting of the Joint Working Group of Experts was held on February 28 –March 2, 2023 in Tashkent, during which experts exchanged views on topical issues of countering the use of the Internet for terrorist and extremist purposes and agreed on approaches to the implementation of new projects and forms of interaction between the competent authorities of the member countries of the association [5].

Joint exercises of the SCO countries on countering terrorist activities on the Internet are being conducted on a systematic basis. In particular, during the period in December 2019 In Xiamen, Fujian Province (Southeastern China) of the joint anti–terrorist exercise to curb the use of the Internet for terrorist, separatist and extremist purposes "Xiamen–2019" [6], the countries of the association, with the coordination of the Regional Anti–Terrorist Structure, practically worked out the issues of applying the provisions of the SCO legal framework regulating joint activities in the field of countering cyberterrorism, collection and recording of electronic evidence, conducting forensic examinations and technical studies, analysis and evaluation of the received digital data.

As a result of the work carried out within the SCO, a proper exchange of operational data on the facts of the spread of terrorist and extremist content on the Internet and a mechanism for taking measures to block it was built, which allowed only in 2019 to delete or restrict access to more than 23 thousand Internet resources containing materials of a terrorist and extremist nature [7].

One of the most important factors in solving the problem of ensuring international information security is also to increase human resources through systematic work on training and advanced training of personnel for anti–terrorist units of the competent structures of the member countries of the association.

In addition, in order to consolidate efforts to counter modern challenges and threats, including in cyberspace, the SCO RATS develops cooperation with international and regional organizations. In particular, memoranda and cooperation agreements were signed with the relevant UN anti–terrorist structures Interpol, the CIS Anti–Terrorist Center, the Secretariat of the Collective Security Treaty Organization, the Secretariat of the Conference on Interaction and Confidence –Building Measures in Asia, the African Center for the Study and Research of Terrorism, etc. In 2021 The Plan of Interaction of the SCO member states on issues of ensuring international information security for 2022–2023, including at the relevant UN sites, has been approved.

It should be noted that today many leading countries of the world and international organizations are concerned about information security issues and in this regard, they pay special attention to information security issues in their documents. However, there is currently no single international legal document on the regulation of Internet relations and related issues.

At the summit of heads of SCO member states held on September 15–16, 2022 in Samarkand under the chairmanship of Uzbekistan, important attention was also paid to information security issues. The SCO Samarkand Declaration adopted at the end of the summit [8] emphasized the key role of the UN in countering threats in the information space, creating a safe, fair and open information space built on the principles of respect for state sovereignty and non-interference in the internal affairs of other countries. The SCO member States categorically opposed the militarization of the ICT sphere and supported the development of universal rules, principles and norms of responsible behavior of states in this area, including welcomed the launch of the development under the auspices of the UN of a comprehensive international convention on countering the use of Information and communication technologies for criminal purposes.

## *Conclusion*

Summing up the foregoing, it can be noted that in order to ensure international information security in the SCO space as a whole, effective mechanisms have been formed to counter the illegal use of modern information and communication technologies.

At the same time, bearing in mind the transnational nature of the information space and the nature of the challenges and threats arising in the digital environment, as well as the importance of information security as a key element of the global security system in the future, active steps are needed to combine international efforts to combat cyberterrorism and to prevent the use of digital space by various destructive forces for hostile acts, as well as to develop a comprehensive international legal instrument to counter cybercrime and ensuring international information security with the central coordinating role of the United Nations.

## *References*

1. SCO RATS website://ecrats.org/ru/news/7096.

2. Yedgorov S. Cyberterrorism as a new global threat // Materials of the republican conference on the topic: features of modern international relations and priorities of the foreign policy of the Republic of Uzbekistan. – Tashkent: UMED, 2017. – p. 111.

3. Here's one tally of the losses from WannaCry ransomware global attack: // www.mcclatchydc.com/news/nation–world/national/national–security/article1524396 39.html.

4. Agreement between the Governments of the member States of the Shanghai Cooperation Organization on cooperation in the field of international information security dated June 16, 2009 // lex.uz/docs/2068478.

5. Website of the SCO Regional Anti–Terrorist Structure: // ecrats.org/ru/press/news/ 2615/.

6. The SCO held exercises to combat cyberterrorism in China. Website of the Chinese Internet Information Center "China.org.cn": // russian.china.org.cn/china/txt/ 2019–12/12/content_75507226.html.

7. Website of the SCO Secretariat://rus.sectsco.org/news/20201111/690868.html.

## Copyrights