Published online: 8 July 2024 DOI: 10.54254/2753-7102/9/2024077

SCO's Cyber Counterterrorism Law Enforcement Cooperation: Current Status, Challenges, and Countermeasures

*Zheng Zhichao [1, a], Lin Haiwen [1, b, *]*

[1] Zhejiang Police College, No. 555 Longyuan Road, Songjiang District, Shanghai, 201600

a. 3363928820@qq.com, b. linhaiwen@zjjcxy.cn
[*] Corresponding author

Abstract. The SCO region has long been a stronghold for terrorism, and the proliferation of the internet has accelerated the development of cyber terrorism. Facing severe cybersecurity threats, the Shanghai Cooperation Organization (SCO) has deepened its cyber counterterrorism cooperation through treaties, joint exercises, and specialized departments, achieving significant results. However, challenges such as insufficient intelligence sharing, lack of professional personnel, and difficulties in law enforcement cooperation remain. Future efforts should adhere to the concept of a community with a shared future in cyberspace, strengthen intelligence sharing, and continue counterterrorism exercises to effectively address the threat of cyber terrorism.

Keywords: Shanghai Cooperation Organization, cyber terrorism, cyber counterterrorism cooperation

With the widespread application of the internet, big data, and cloud computing, cyber terrorism is becoming increasingly severe. Terrorists are exploring cyber technologies to launch cyberattacks against infrastructure or use virtual platforms to spread terror rumors, severely disrupting national security and social order. Due to the virtual and borderless nature of cyberspace, it is impossible to eradicate cyber terrorism relying solely on the efforts of a single country. Only by building international consensus and strengthening cyber counterterrorism cooperation can effective governance of cyberspace be achieved. As a regional security organization, the SCO faces severe cyber terrorism threats, making the analysis of its cyber counterterrorism law enforcement cooperation's current status, challenges, and countermeasures of great theoretical and practical significance.

1. Terrorism Headquarters

1.1. Terrorism Headquarters

The Shanghai Cooperation Organization (SCO) currently has nine member states, the vast majority of which are located in South Asia and Central Asia and have long been the headquarters for international terrorist organizations. Since the beginning of this century, the number of terrorist attacks in member countries accounts for 10%-36% of the global total, and the overall situation concerning terrorism is extremely severe[1]. In the 2023 ranking of countries affected by terrorism, Pakistan ranks fourth globally, India is fourteenth, and Russia is thirty-fifth[1]. Long-term exposure to separatist and extremist ideologies has led to some ethnic groups inciting opposition and hatred in pursuit of their own interests, creating turmoil that severely disrupts social order and government rule. The turbulent environment has become a "crime lowland" for the rapid development of terrorist organizations.

1.2. Increase in Internet Penetration Rate

The member states of the Shanghai Cooperation Organization (SCO) place a high emphasis on the development of information technology, with a rapid increase in internet penetration and the number of users in recent years. By the end of 2023, the scale of internet users in China reached 1.092 billion, an increase of 24.8 million new netizens compared to December 2022, with an internet penetration rate of 77.5%[2]. The Prime Minister of Kazakhstan, Askar Mamin, stated in 2021 that the country's internet

[1] Reference:<GLOBAL TERRORISM INDEX2024>, file://C:/Users/ASUS/Downloads/GTI-2024-web-290224.pdf
[2] China's Internet User Scale Reaches 1.092 Billion People, https://www.gov.cn/yaowen/liebiao/202403/content_6940952.htm

penetration rate had reached 99%[3], and he expected full coverage of 5G networks by 2024. Kyrgyzstan ranks first in the Central Asian region in terms of mobile communication penetration rate[4]—with a population of 6.58 million people, there are 10.23 million SIM cards, an astonishing 155.6%[5]. While convenient and efficient information technology has made life more convenient, it has also sown significant security risks.

1.3. Rapid Development of Cyber Terrorism

Cyber terrorism is the concentrated expression of terrorism in cyberspace, a product of the continuous evolution, integration, interweaving, and infiltration of terrorism in the digital realm. The international community's pressure on the physical living space of traditional terrorism has forced it to spread more rapidly and aggressively into cyber terrorism[2].The "East Turkestan Islamic Movement" (ETIM) has established the "Voice of Islam Propaganda Center," which has disseminated a large number of violent and extremist audio and video materials on social media platforms. The "Islamic State" has developed a simulation game called "The Sword Rings Out," attempting to intensify and recruit new members, especially young people to join[3].In 2015, less than a year after the declaration of the Islamic State, 2,000-4,000 Central Asian terrorist fighters have been recruited[4], and the participation of women and young people in "jihadist" extremist terrorist activities has become increasingly prominent.

2. Current Status of SCO Cyber Counterterrorism

Counterterrorism has always been a priority for the Shanghai Cooperation Organization (SCO). Since its establishment in 2001, the SCO has achieved significant results in the field of cyber counterterrorism cooperation. Over the past two decades, the primary cooperation models developed include treaty-based, mechanism-based, and institution-based approaches. The evolution from treaties to mechanisms, and from mechanisms to institutions, signifies a continuous upgrade in cooperation models, an expansion of cooperation content, and a strengthening of cooperative relationships. These efforts have significantly curbed cyber terrorism within SCO member states and hold great practical significance for maintaining regional cyberspace security.

2.1. Treaty-Based Cooperation

The signing of treaties has been integral to the entire process of SCO's cyber counterterrorism cooperation, and in recent years, it has been discussed as a priority. The 2020 "Statement on Combating the Use of the Internet and Other Channels to Spread Terrorist Ideology"[6] was the first statement document directly themed on "cyber terrorism." The 2022 and 2023 Council of Heads of State meetings respectively issued the "Samarkand Declaration"7 and the "New Delhi Declaration,"8 both emphasizing the need to "take proactive measures to cut off terrorist financing channels and curb the spread of terrorist ideology."9 The "Statement on Cooperation in Combating Extremism Leading to Terrorism" further required member states to "work together, according to their domestic laws, to block and remove extremist and terrorist content online and take legal action against identified individuals and entities." This series of treaty documents has consolidated consensus among member states, placing the fight against cyber terrorism at the core of counterterrorism efforts and laying a solid foundation for deepening the implementation of SCO cyber counterterrorism cooperation.

2.2. Action-Based Cooperation

The SCO has held three cyber counterterrorism exercises in Xiamen, China, in October 2015, December 2017, and December 2019. These exercises combined simulated actual combat with theoretical drills to realistically reproduce cyber terrorism activities[10]. Representatives from participating member states conducted investigations based on online clues according to their national laws, located members of terrorist organizations, examined and collected evidence from electronic devices, and organized coordinated capture operations. The third SCO cyber counterterrorism joint exercise in China yielded significant results, enhancing mutual trust among member states and deepening cooperation in intelligence exchange, action coordination, and capacity building. From 2016 to 2017, SCO member states collectively blocked over 100,000 websites that hosted more than 4 million pieces of content promoting terrorism and extremism[11].

---

[3] Kazakhstan's Internet Penetration Rate Has Reached 99%, https://cn.inform.kz/news/99_a3749738/

[4] The 5G network in Kazakhstan will cover the whole country by 2024, https://cn.inform.kz/news/2024-5g_a3963412/

[5] Today let's talk about the internet speed in Central Asia, https://new.qq.com/rain/a/20211129A0D1SF00

[6] The full name is "Declaration of the Council of Heads of State of the Shanghai Cooperation Organization Member States on Combating the Dissemination of Terrorism, Separatism, and Extremism Ideologies through the Internet and Other Channels."

[7] The full name is "Samarkand Declaration of the Council of Heads of State of the Shanghai Cooperation Organization Member States."

[8] The full name is "New Delhi Declaration of the Council of Heads of State of the Shanghai Cooperation Organization Member States."

[9] The full name is "Declaration of the Council of Heads of State of the Shanghai Cooperation Organization Member States on Cooperation in Combating Radicalization Leading to Terrorism, Separatism, and Extremism."

[10] The Third SCO Cyber Anti-Terrorism Joint Exercise Held in China, http://world.people.com.cn/n1/2019/1212/c1002-31503716.html

[11] Exclusive Interview: SCO Anti-Terrorism Efforts Are Highly Effective, https://www.gov.cn/xinwen/2018-05/09/content_5289477.htm

2.3. Institutional Cooperation

In 2004, the SCO Regional Anti-Terrorist Structure (RATS) was established as a permanent institution to coordinate counterterrorism efforts. In 2006, the International Information Security Experts Group was formed to develop an action plan for information security. In 2015, the RATS news center announced the establishment of a collaborative mechanism to prevent cyber terrorism threats within its organizational structure. This mechanism includes monitoring the uploading of photos, audio, and video by extremist organizations, as well as the online recruitment of individuals into terrorist groups[12]. The "Samarkand Declaration of the SCO Heads of State Council" proposed the establishment of an SCO Information Security Center. During the interdepartmental consultation meeting held in Almaty in 2023, the overall concept, organizational structure, staffing, and mission objectives of the Information Security Center were further clarified. The establishment of this center is expected to play a significant role in quickly responding to cyber terrorism threats and maintaining the security of the information space within the SCO region13.

3. The Enforcement Dilemma in Cyber Counter-Terrorism Cooperation

3.1. Lack of Intelligence Information Sharing

Intelligence information sharing is an important indicator to measure the depth of counter-terrorism cooperation. Article 6 of the "Agreement on the Regional Anti-Terrorism Structure"14 stipulates that the functions of the institution include establishing a database and providing information upon request from the competent authorities of the parties. Although there are already channels and platforms for information communication, for various reasons, the goal of real-time sharing of counter-terrorism intelligence has not yet been achieved. The multitude of languages in the SCO region undoubtedly increases the difficulty of collecting and exchanging intelligence information. Russian and Chinese are the working languages of the SCO, but the use of Chinese is far less frequent than Russian. National languages other than Russian are also easily overlooked in the intelligence collection process[5]. With the addition of Pakistan, India, and Iran, the internal language environment of the organization has become more complex, increasing translation pressure and affecting communication efficiency. In addition, the scope of intelligence exchange is extremely limited, and more detailed information such as the personal life and social relations of suspected terrorists is not within the scope of intelligence exchange, which seriously restricts the depth of cooperation[6].

3.2. Lack of Cyber Anti-Terrorism Teams

Conducting cyber anti-terrorism cooperation requires not only individuals who are proficient in cybersecurity knowledge and possess counter-terrorism combat skills but also those who can communicate with foreign anti-terrorism law enforcement personnel in foreign languages. At present, the scarcity of such versatile talents is extremely rare[7]. Taking Pakistan as an example, its national institution responsible for cybersecurity—the National Cyber Security Incident Response Team—only operates selectively at the organizational level of the public and defense sectors[8]. The shortage of talents also leads to the obstruction of "group formation" within the organization. The SCO's regional anti-terrorism institution lacks a transnational joint cyber anti-terrorism law enforcement team dedicated to the prevention and crackdown of cyber terrorism activities. In contrast, NATO established the Cooperative Cyber Defense Center of Excellence in 2007, and Europol established the Internet Referral Unit in July 2015, specifically responsible for combating the promotion of terrorism and extremism on the Internet. The "Benevolence" special action team under the department has carried out multiple special operations to clean up and punish cyber terrorism-related information[9].

3.3. Difficulties in Anti-Terrorism Law Enforcement Cooperation

The main battlefield of cyber terrorism is the online virtual platform, where terrorists can undermine the security of other countries without crossing a national border. However, cooperation between countries faces a lot of resistance. Unlike traditional terrorism, the ambiguity of boundaries leads to the uncertainty of jurisdiction[10]. Cyber anti-terrorism cooperation should first solve the issue of the attribution of jurisdiction. Judicial cooperation involves a country's judicial sovereignty, which is mainly based on treaties signed by both parties. However, the treaty system between China and some countries such as India and Uzbekistan is not perfect. On the other hand, different countries have different legal regulations on cyber terrorism, and there is a possibility that cooperation cannot be carried out because it does not meet the "dual crime" principle. Cyber terrorism is mostly fragile electronic evidence, which is easily destroyed, forged, or tampered with, weakening its integrity and greatly reducing its reliability and evidential power. Because it involves multiple countries, the coordination is difficult, the case investigation takes a long time, and

[12] SCO Regional Anti-Terrorism Body: Member Countries Have Established Cyber Anti-Terrorism Cooperation Mechanism, https://news.sina.com.cn/w/2015-07-09/161632090725.shtml

[13] SCO Member Countries Hold Inter-Departmental Consultations on the Establishment of an Information Security Center，https://chn.sectsco.org/20230915/956639.html

[14] The full name is "Agreement Among the SCO Member States on the Regional Anti-Terrorist Structure".

in the end, very few terrorists are brought to justice, which is difficult to achieve the purpose of effectively combating and deterring cyber terrorism activities[11].

4. Development Path for SCO Cyber Counterterrorism

4.1. Adhering to the Concept of a "Community of Shared Future in Cyberspace"

On December 16, 2015, General Secretary Xi Jinping, during the Second World Internet Conference, emphasized that "countries should work together to build a community of shared future in cyberspace." In the face of cyberterrorism threats, no country can tackle this issue alone. SCO member states need to unify their consensus, work hand-in-hand to address this global problem. Due to the current differences in national legislations, deepening cybersecurity cooperation requires reasonably ceding some sovereignty while maintaining national sovereignty. This will accelerate collaborative governance in cyberspace, promote the cooperative use of cyber resources[12], and foster the secure and stable development of cyberspace, aligning with the spirit of the "Shanghai Spirit."

4.2. Strengthening Cyber Counterterrorism Intelligence Work

Information leadership and intelligence support are key points in the counterterrorism strategies of many countries. Intelligence plays a predictive, monitoring, forward-looking, and leading role in cyber counterterrorism efforts. The regional anti-terrorist institution should fully leverage its role as an intelligence information hub. Member states should enhance the timeliness and accuracy of intelligence sharing, strengthen analysis and early warning capabilities, and prevent the further spread of cyberterrorism.

4.3. Continuously Conducting Cyber Counterterrorism Exercises

Cyber counterterrorism exercises have achieved significant results. However, due to various reasons, the fourth exercise has not been conducted. Future exercises should focus on the latest developments in cyberterrorism. The frequency of exercises should be increased, as the current biennial joint exercises have too long an interval. With the rapid development of information technology, more frequent exercises will help counterterrorism personnel stay abreast of new forms and characteristics of cyberterrorism and prepare timely responses. SCO's cyber counterterrorism efforts have traditionally focused on "instrumental" cyberterrorism, which uses the internet as a tool for propaganda and recruitment. The first three exercises also reflected this focus. There has yet to be preparation for "target-oriented" cyberterrorism. It cannot be ruled out that terrorist organizations could acquire advanced technologies and launch cyber-attacks on critical infrastructure. Therefore, the scope of the exercises needs to be expanded.

References

[1] Wang, D., & Lu, P. (2023). Analysis and Countermeasures of Terrorist Attacks in SCO Member States—Based on GTD Terrorism Database. *Journal of Yunnan Police Officer Academy*, (03), 58-67. (p.64)
[2] Qin, G. (2020). The Threats and Responses of Cyber Terrorism under the Belt and Road Initiative. *Journal of China Criminal Police Academy*, (05), 22-31. (p.22)
[3] Andini, O.P. (2021). Cyber Terrorism Criminal Acts in the Perspective of Transnational Organized Crime. *Unnes Law Journal*, 7(2), 333-346. (p.341, ACM)
[4] Su, C. (2017). The Extension of ISIS Influence in Central Asia: A Realistic Analysis and Possibility Assessment. *Russian Studies Journal*, 7(03), 69-76. (p.75)
[5] Zhang, J. (Year). International Police Cooperation in Counterterrorism—From the Perspective of Shanghai Cooperation Organization Regional Cooperation. (p.258)
[6] Meng, L. (2018). An Analysis of International Cooperation in Cyber Counterterrorism. *Police Studies Research*, (06), 42-48. (p.47)
[7] Sha, J., & Zeng, F. (2022). Research on the Dilemmas and Countermeasures of China's Counter-Cyberterrorism from the Perspective of International Cooperation. *Network Security Technology and Application*, (11), 151-152. (p.152)
[8] Ji, S., & Wang, H. (2022). An Analysis of Pakistan's National Cybersecurity Policy 2021. *China Information Security*, (02), 88-91. (p.88)
[9] Wang, L. (2018). Research on International Cooperation in China's Fight Against Cyberterrorism. *China People's Public Security University*. (p.30)
[10] Meng, L. (2018). An Analysis of International Cooperation in Cyber Counterterrorism. *Police Studies Research*, (06), 42-48. (p.47)
[11] Wang, X. (2017). Research on SCO's Countermeasures Against Cyberterrorism. *China People's Public Security University*. (p.14)
[12] Du, J. (2019). Research on Countermeasures Against Cyberterrorism—Based on the Maintenance and Concession of National Cyber Sovereignty. *Journal of Nanning Normal University (Philosophy and Social Sciences Edition)*, 40(06), 163-172. (p.171)