Frontiers in Business, Economics and Management
ISSN: 2766-824X | Vol. 15, No. 2, 2024

The Role of the SCO in the Progressive Development of International Legal Norms in the Field Of Information Security

Yuxi Hu *

Belarusian State University, Faculty of law, 220070, Minsk, Belarus
* **Corresponding author**: Yuxi Hu (Email: xier613@gmail.com)

Abstract: This paper aims to explore the potential of regional organizations to play a constructive role in addressing global cybersecurity challenges. This paper will examine the legal framework established by the SCO to address the challenges posed by cyber threats and assess its effectiveness in promoting regional cyber security. During the discussion of the SCO, specific cases will be provided and the challenges and solutions of cooperation in different areas will be presented through the analysis of actual cases. This argumentative method based on actual cases enhances the credibility and practicability of the article. In general, this paper presents the legal framework established by the SCO to address the challenges posed by cyber threats and assesses its effectiveness in promoting regional cyber security. The research results and arguments in this paper provide useful references for the international community and have important theoretical and practical implications for promoting global cooperation and achieving common development.

Keywords: Information security, Foreign policy, Cooperation, SCO, UN, Information warfare, Cyber warfare, Cyber power.

1. Introduction

Information security is the practice of protecting information from unauthorized access, use, modification or destruction. In today's world, information is increasingly stored, processed and transmitted digitally, which is very important to ensure the confidentiality, integrity and availability of data. However, in the face of ever-changing threats, technologies and regulations, information security faces many challenges and risks.

The main challenges and risks of information security include cyber-attacks which aim to disrupt or harm information systems, human factors such as negligent behaviors that can compromise security, and technological changes that introduce new vulnerabilities. Additionally, regulatory compliance mandates impose complexities and costs on organizations to uphold information security standards and avoid penalties for non-compliance.

In the traditional sense, the connotation of network threat refers to the use of technical means, taking advantage of the loopholes, defects or weaknesses of the target object, and taking measures such as detection, penetration, invasion, privilege promotion, theft and tampering to destroy it. Confidentiality, integrity and security of the target object. Availability and other security attributes. For example, invading the database to illegally obtain personal data and sensitive information, implanting Trojan virus into user terminals to achieve remote control purposes, or launching a large-scale denial of service attack to interrupt network application services.

Cyber threats have evolved beyond direct attacks on networks to encompass utilizing cyberspace for political control and competitive advantage at an international level, influencing economic, military, cultural, and public opinion spheres. This study explores how the evolving landscape of international cyber threats, shifting from traditional sabotage to strategic control of cyberspace for political and economic gain, highlights the importance of the Shanghai Cooperation Organization's role in shaping international legal norms for information security to address contemporary challenges and promote global stability.

2. Legal Mechanisms to Ensure Information Security (Domestic and International)

Data Security Law plays a crucial role in safeguarding people's rights in the digital economy and promoting the rational use of data for innovation.

As a new type of trading commodity, the value evaluation, payment method and delivery channel of data trading are very different from traditional physical commodity trading. All aspects of the transaction process need to be supervised by network security, especially whether the data goods have privacy. Leaks, illegal transactions, information fraud and other illegal acts. In order to solve this problem, it is necessary to study the key technologies such as identity authentication of transaction parties, content compliance review, trustworthy traceability, transaction marking, payment security, etc., so as to promote the legal and compliant use of data and realize data transaction, economic operation and social circulation. Deep integration.

Legal mechanism is one of the tools to ensure domestic and international information security. Legal mechanisms include laws, regulations, standards, policies, guidelines and agreements that define the rights and obligations of information security stakeholders (such as countries, organizations and individuals). The legal mechanism also provides a basis for the establishment of accountability and enforcement mechanisms for information security violations. Some examples of legal mechanisms to ensure domestic information security include:

(1) Data protection law regulating the collection,

processing, storage and transmission of personal data by public and private entities. For example, the Law of Belarus on Information, Informatization and Information Protection (2008) provides the legal framework for data protection in Belarus.

(2) Cybercrime law criminalizes various forms of malicious activities against information and information systems, such as hacking, phishing, malware, denial of service attacks and identity theft. For example, the Criminal Code of Russia (1996) contains several articles concerning cybercrime and sanctions.

(3) Network security laws stipulate the roles and responsibilities of government agencies and other participants in preventing, detecting, responding to and recovering from network events. For example, Ukraine's Law on the Basic Principles of Cybersecurity (2017) defines the national cybersecurity system and its components.

(4) The national cyber security strategy outlines the vision, objectives, goals, principles and actions to enhance the national cyber security situation and resilience. For example, the Estonian Cyber Security Strategy for 2019-2022 (2018) defines the strategic priorities and measures to strengthen Estonia's cyber capabilities and cooperation [1].

(5) Industry regulations that set minimum requirements and best practices for information security in specific industries (such as finance, energy, telecommunications and health). For example, the European Union Network and Information System Security Directive (NIS Directive) (2016) established a common security level for key infrastructure operators in the European Union.

Some examples of legal mechanisms to ensure information security at the international level include:

(1) International conventions that stipulate the binding obligations of countries to cooperate in combating cyber-crime and protecting cyber human rights, such as the Council of Europe Convention on Cybercrime (Budapest Convention) (2001) and the International Covenant on Civil and Political Rights (ICCPR) (1966).

(2) Regional frameworks for coordinating legal methods and standards for information security among regional partners, such as the EU General Data Protection Regulation (GDPR) (2016) and the African Union Convention on Cybersecurity and Personal Data Protection (Malabo Convention) (2014).

(3) Bilateral or multilateral agreements, such as MLAT and CBM, that promote information exchange and help to deal with cross-border cyber threats and incidents. For example, the US-EU Umbrella Agreement (2016) provides a framework for transatlantic data transmission for law enforcement purposes.

(4) Non-binding instruments that provide guidance and suggestions for improving information security governance and cooperation at the global level, such as the United Nations General Assembly resolution on the development of information and telecommunications in the context of international security (UNGA Res) and the report of the United Nations Group of Governmental Experts on promoting responsible state behavior in cyberspace in the context of international security (UNGGE). For example, the 2015 UNGGE report contains a set of voluntary norms for responsible state behavior in cyberspace [2].

The current state of development in both domestic and international information security legal mechanisms involves a mix of binding conventions, regional regulations, bilateral agreements, and non-binding instruments, with the key to addressing and overcoming this state lying in enhancing cooperation, promoting responsible state behavior, and establishing comprehensive frameworks to combat cyber threats effectively.

3. Shanghai Cooperation Organization's Contribution to Information Security

3.1. The Effectiveness Analysis of Information Security Activities of the Shanghai Cooperation Organization

The Shanghai Cooperation Organization (SCO) works towards enhancing information security cooperation among its member and observer countries as part of its broader aims in security, economy, culture, and humanitarian affairs.

The Shanghai Cooperation Organization (SCO) has played a significant role in advancing international information security (IIS) efforts through various initiatives and collaborations among its member States. In 2006, the SCO elevated the importance of IIS by officially addressing the issue on its website and subsequently adopting the Statement of Heads of SCO Member States on IIS during the summit in Shanghai. This statement underscored the shared concern among member States about the misuse of information for criminal, terrorist, and military purposes, emphasizing the need for collective action within the SCO framework.

A pivotal outcome of the SCO's commitment to IIS was the adoption of the Agreement between the Governments of the Shanghai Cooperation Organization Member States on Safeguarding International Information Security during the Yekaterinburg Summit in June 2009. This agreement, which came into effect on January 5, 2012, facilitated cooperation among SCO member States in combating threats posed by the misuse of information and communication technologies for terrorism and criminal activities. It also focused on enhancing information sharing on national cyber security legislation and strengthening the international legal framework for cooperation on IIS within the SCO.

Furthermore, the SCO's efforts have extended to promoting international information security on the global stage, notably within the United Nations. By championing initiatives to include IIS on the UN agenda, the SCO highlighted the importance of responsible behavior in information space. Although initial efforts faced criticism and revisions were needed to align with expert recommendations, the SCO persisted in advocating for enhanced IIS measures in collaboration with other member States.

The organization has also taken concrete steps to bolster its capabilities in responding to cyber threats and security challenges by establishing regional anti-terrorism agencies, the SCO Cyber Security Bureau, and mechanisms like the SCO anti-terrorism convention. Through joint exercises such as the "Peace Mission" anti-terrorism series and the "Cyber Shield" exercise, as well as hosting the SCO Cyber Security Forum, the SCO has focused on enhancing preparedness and interoperability among member States to effectively address cyber incidents.

Overall, the Shanghai Cooperation Organization's dedicated efforts and contributions in the realm of information security have not only strengthened cooperation among its member States but also underscored the organization's commitment to fostering a secure and resilient digital environment.

3.2. Limitations and Challenges of the SCO in the Field Of Confidence and Security

However, the SCO still faces some challenges and limitations in response and effectiveness to cyber-attacks and other security challenges, such as:

(1) The lack of a common definition and understanding of network security among member States may lead to differences in methods and interests in dealing with network problems [3].

(2) The legal and institutional framework and mechanism for ensuring compliance and implementation of SCO agreements and decisions on cybersecurity matters are insufficient [4].

(3) Lack of resources and ability to monitor and respond to network threats and events in a timely and effective manner [5].

(4) Potential conflicts and tensions between its member States or with other actors on network-related issues such as sovereignty, territorial disputes, human rights and trade [6].

It is necessary to strike a balance between the goal of cyber security and the goal of economic development and digitalization, as well as respect for international laws and norms. Evaluate the response of the Shanghai Cooperation Organization to cyber-attacks [7].

The SCO has been facing more and more cyber threats from different sources, such as state-sponsored hackers, terrorist organizations, criminal organizations and hacker activists.

The SCO has taken a number of measures to enhance network resilience and cooperation, such as: In 2005, the Information Security Working Group was established, and in 2013, the Cybercrime Group was established. In 2017, the convention on combating extremism was signed, including provisions on preventing and combating cyber extremism. "Surrey-Alca-Anti-Terrorism 2019" and other joint cyber defense and anti-terrorism exercises. Develop a common legal framework and technical standards for network security and data protection among member States. Promote cooperation with the ASEAN Regional Forum and other regional and international organizations such as the United Nations on network issues. Dialogue and coordination.

The Shanghai Cooperation Organization (SCO) influences the formulation of international legal instruments on information security through establishing common norms emphasizing respect for sovereignty, peaceful use of ICT, prevention of cybercrime and terrorism, and promotion of the digital economy. The SCO has set up a consultation mechanism among member States and collaborates with organizations like CSTO, ASEAN, BRICS, and the UN, facilitating dialogue through platforms like the International Information Security Forum and SCO Youth Council. Through joint exercises, capacity-building projects, and information sharing, the SCO actively addresses cyber threats like cyber-crime and terrorism, enhancing information security among its member States [8]. Some important actions such as: By exchanging views and best practices on cyber threats and challenges, the Shanghai Cooperation Organization aims to develop a network security, common methods, and standards to enhance mutual trust and confidence between member States and other partners. The organization works towards promoting regional and global stability and security by preventing and combating cyber-crime, cyber terrorism, and cyber warfare while supporting international efforts to address these issues. The SCO also strives to foster cooperation and coordination among relevant institutions and agencies of member States and other partners in information security fields such as law enforcement, intelligence, national defense, and diplomacy. Additionally, the organization supports member States and partners in capacity building and technical assistance in information security by providing training, education, research and development opportunities, and facilitating access to advanced technology and equipment. Moreover, the SCO endeavors to promote dialogue and collaboration with the United Nations, the European Union, the Association of Southeast Asian Nations, the Organization of American States, the African Union, and other regional and international organizations in the realm of information security to address common problems, challenges, and opportunities in cyberspace [9].

4. Shanghai Cooperation Prospects Organizations That Ensure Information Security

4.1. Analysis of the Promising Measures That the SCO May Take In International Legal Support for Information Security

One of the main challenges faced by the Shanghai Cooperation Organization (SCO) is navigating the conflicts of interests among its member States regarding information security issues. The SCO, a regional organization dedicated to fostering cooperation and stability in Eurasia across various sectors including security, economy, culture, and humanitarian affairs, encounters divergent perspectives within its member countries on addressing the challenges and opportunities arising from the digital revolution. Countries like China and Russia advocate for a state-centered and restrictive information governance model characterized by stringent content control, online surveillance, and stifling of dissenting voices. Conversely, nations such as India and Pakistan advocate for a more open and inclusive approach that upholds human rights and freedoms, emphasizing data privacy, information flow, and diversity in the digital realm. These contrasting viewpoints have impeded the establishment of a unified strategy and framework for information security within the SCO.

To overcome these dissonances, the SCO must adopt a pragmatic and flexible stance, respecting the diversity and sovereignty of its member States while seeking common ground for mutual benefit. The organization should prioritize addressing pressing challenges common to all member States, such as cyber-crime, cyber terrorism, and cyber warfare, along with safeguarding against cyber espionage and attacks on critical infrastructure. By establishing mechanisms for information sharing and cyber incident coordination, devising a cohesive legal framework against cyber-crimes, enhancing member States' capabilities to prevent and respond to cyber

threats, and conducting joint exercises on network defense, the SCO can bolster its collective cybersecurity efforts. Additionally, fostering dialogue and knowledge exchange among member States to find a harmonious balance between national security imperatives and upholding human rights and freedoms in the digital sphere is crucial for effective information security governance.

Furthermore, the SCO should strengthen collaborations with key international bodies like the United Nations, European Union, Association of Southeast Asian Nations, and the Organization for Security and Cooperation in Europe to align agendas and values in the realm of information security. This cooperative approach will contribute to building a safer, more stable, and prosperous information environment for SCO member countries and the wider global community.

4.2. Overcoming the Conflict of Interests of SCO Member States on Information Security Issues

The information security challenges within the Shanghai Cooperation Organization (SCO) present opportunities for enhanced cooperation. Member States must address the "digital divide" by bridging discrepancies in technology and governance capabilities to effectively combat security risks.

First, Embracing cooperation from a regional security and developmental perspective, leveraging technologies like 5G and artificial intelligence, and pooling resources to establish robust information protection systems and efficient exchange mechanisms are crucial steps. China, Russia, and India, with their significant expertise and resources, should lead in strengthening legal frameworks, technical capabilities, and operational readiness to build a secure and collaborative information security network within the SCO. By fostering collaboration, innovation, and shared responsibility, member countries can collectively bolster information security and navigate the digital landscape with resilience and unity.

For example, the SCO can regularly organize consultations and seminars on information security issues, build a platform for civil society to participate in digital rights issues, and support confidence-building measures and information security measures through information security codes of conduct or declarations of principles. A code of responsible behavior in cyberspace. The SCO should also strengthen cooperation with the United Nations, the European Union, the Association of Southeast Asian Nations, the Organization for Security and Cooperation and other regional and international organizations with common goals and values in the field of information security. Operation in Europe (OSCE). The SCO's move will contribute to building a safer, more stable and prosperous information environment for member States and the world [10].

The second is to promote regional digital governance and build an information security community. It requires: member States should speed up the construction of "soft" and "hard" digital infrastructure and strive to narrow the technology gap; Strengthen communication and coordination among governments, enterprises and the private sector at all levels to promote the integrated development of digital platforms and digital strategies in various countries; Countries should also strive to reach consensus on issues such as regulatory system, digital rules, data sharing and data security protection, so as to create favorable conditions for building a unified information data platform and information security community of the SCO.

The third is to improve the information security system and mechanism. One of the most urgent tasks facing the SCO is to legalize and institutionalize the consensus on information security cooperation among member States and establish an efficient and perfect information security cooperation mechanism. Ideally, countries should cooperate to establish a comprehensive and systematic information security cooperation mechanism: establish a high-level consultation mechanism on information security, add more information security-related content at the SCO summit, and review it regular.

4.3. Incorporation of International Law in the Field Of Information Security into the National Legislation of SCO Member States

Some possible ways to solve the conflicts of interest of SCO member States on information security issues are:

(1) Establish common principles and normative framework for responsible state behavior in cyberspace in accordance with international law and existing agreements of the SCO.

(2) Strengthen cooperation and coordination among SCO member States in the prevention, detection, response and mitigation of cyber threats, network capacity building and trust measures.

(3) Promote dialogue and exchange of best practices among SCO member States on information security such as data protection, privacy, cybercrime, cyber terrorism, digital economy and digital sovereignty.

(4) Develop joint initiatives and projects within the framework of the SCO to address specific information security challenges and opportunities, such as combating cyber extremism and radicalization, promoting digital inclusion and innovation, and supporting the development of secure and flexible digital infrastructure.

(5) Strengthen partnership and cooperation with other regional and international organizations and relevant stakeholders in the private sector, civil society and academia on information security issues of common concern [11].

In short, organizational flexibility management, encompassing network security, emphasizes the significance of assessing network risks comprehensively and implementing preventive measures while establishing procedures for responding to threats to ensure business continuity. Risk reduction in network security is a nuanced process that requires both avoidance and effective post-attack recovery strategies. Developing and regularly testing rigorous disaster recovery procedures tailored to the organization's risk tolerance, resource availability, and business constraints are essential for restoring normal operations effectively. Business continuity planning and risk management, aligned with strategic parameters and organizational needs, serve as crucial components in fortifying an organization's resilience against physical and network threats.

5. Conclusion

The Shanghai Cooperation Organization (SCO) is a regional multilateral organization, which aims to promote cooperation and dialogue among member States on various

issues such as information security and international law. The SCO has adopted a number of documents and initiatives to deal with the challenges and threats brought by the abuse of information and communication technology (ICT), the effectiveness of the SCO in promoting information security and promoting international law in this field is still limited by the following factors:

There is insufficient coordination and cooperation between SCO member States and other relevant actors and stakeholders (such as other regional and international organizations, civil society, academia and the private sector) on information security issues.

The capacity and resources of SCO member States are limited, so it is impossible to effectively implement and implement the existing SCO information security documents and initiatives, and it is also impossible to formulate new documents and initiatives that reflect the changing nature and complexity of the problem.

In order to improve the effectiveness of the Shanghai Cooperation Organization in promoting information security and promoting international law in this field, the following suggestions are put forward:

The SCO should strengthen coordination and cooperation with other relevant parties and stakeholders on information security issues within and outside the SCO framework. This will enable the Shanghai Cooperation Organization to give full play to its comparative advantages and complementarities with other regional and international organizations, civil society, academia and the private sector, and contribute to the development of more inclusive and cooperative global governance of cyberspace.

The SCO should strengthen its capacity and resources, effectively implement and implement existing information security documents and initiatives, and formulate new documents and initiatives that reflect the changing nature and complexity of the problem. This requires more political will and commitment from SCO member States and more technical assistance and support from external partners.

To sum up, in order to ensure the international information security of the entire SCO space, an effective mechanism has been formed to crack down on the illegal use of modern information and communication technologies.

References

[1] Resolution of the UN General Assembly (A/RES/53/70)of December 4,1998 “A chievement in the ield bf informatization and telecommunications in the conrext of intsrnational security //Official website of the UN [Electronic resource]. – Mode of access: http://www.un.org/ru. – Date of access: 02/28/2023.

[2] Resolution of the UN General Assembly A/RES/65/41) of December 8, 2010" Achievements in the field of informatization and communications in the context of international security [Electronic resource]. – Mode of access. http:/www.scrf.go v.ru/news/720.html$http. – Date of access: 03/02/2023.

[3] Recommendation CM /Rec (2011) 8 of the Committee of Ministers to Member States on the protection and promotion of the universal character, integrity and openness of the Internet (Adopted by the Committee of Ministers on September (21,2011) [Electronic resource].— Mode of access. http://hronline.org.ua/npanel/webdata/299/12_rekomendatsiya-(2011)8.pdf. – Date of access: 01/03/2023.

[4] CIS Model Law “On International Inform tion Exchange (Adopted by the Resolution of the Interparliamentary Assembly of the CIS Member States dated March 26,2002 No.19-7)//Information Bulletin of the Interparliamentary Assembly of the CIS Member States.2002.No.29 [Electronic resource] – Mode of access: http://base.garant.ru/2569410/. – Date of access: 26/03/2002.

[5] Institute of Information Security (Resolution of the IPA CIS dated November28, 2014No.41-15) [Electronic resource] – Mode of access: http://www.parliament.am/library/modelayin. – Date of access: 03/06/2021.

[6] Agreement between the Government of the Russian Federation and the Government the Government of the Republic of India on cooperation in the field of ensuring international information and communication technologies (October15, 2016) Official portal of the Ministry of Foreign Affairs of the Russian Federation. [Electronic resource] – Mode of access: http:www.mid.ru/foreign policy/intenational contracts/2 contract/-/storage-viewer/bilateral/peye-9SL667. – Date of access: 03/06/2023.

[7] Agapov PV, Efremova M. A. International legal framework for ensuring information secbtity of participants in the Commonwealth of Independent States // Legal Science and Law Ehforcement Practice. 2015. Na (31). – pp. 176-182.

[8] Arlamov E. A., Panasyuk G. O. Analysis of the state of information security dangers in modern Russia //Economics and management of innovative technologies. (2016 No.12) [Electronic resource] – Mode of access: http://ekonomika.snaukau2016A2/13291. – Date of access: 03/21/2013..

[9] Molchanov N. A, Matevosova E.K. Doctrine of information security of the Russian Federation(legislative novelty)//Actual problems of Russian law.2017. No.2.(75). – pp. 159-165.

[10] Okhrimenko. S.A., Cherney G. A. Security Threats to Automated Information Systems(Program Abuses) // Scientific and Technical Information.Series1, Organization and methodology of information work. 1996. – No.5.

[11] ITU Global Cybersecurity Agenda. Basis for international cooperation in the field of cybersecurity [Electronic resource]. – Mode of access: http://www.ifap ru/pr/2008/080908.pdf. – Date of access: 02.03.2023.