Cyber security Cooperation within the Shanghai Cooperation Organization (SCO)

Dr. Ahmed Mohamed Salah Eldin El Alfy

Lecturer at the Public International Law department at the faculty of law, Beni Suef University.

Abstract:

The contemporary international system is undergoing profound transformation, characterized by deepening globalization and rapid technological advancements. While enhancing interconnectedness and facilitating cooperation on shared challenges, these trends simultaneously generate new vulnerabilities and transnational threats. Concepts such as security communities and the trend of regionalism gain prominence in this context, as states increasingly seek cooperative frameworks to manage risks and foster stability. The Shanghai Cooperation Organization (SCO) represents a significant manifestation of this contemporary regionalism, particularly within the Eurasian geopolitical landscape. Evolving from border dispute resolution, the SCO has developed into a multi-purpose organization addressing political, economic, and security issues.

Member states of the SCO confront numerous emerging security challenges, among which cyber threats, including cyber terrorism, are increasingly prominent. Addressing these necessitates significant collaborative effort, especially given major cyber incidents experienced by several member states. Despite the growing recognition of cyber threats and considerable scholarly attention to the SCO's broader security agenda, a specific gap exists in the literature concerning a detailed analysis of the *mechanisms, effectiveness, and limitations* of the SCO's collective response framework dedicated to cyber security.

(ISSN: 2537 - 0758)

This study aims to fill this gap by providing a focused analysis of the SCO's engagement with cyber security issues. Its significance stems from the escalating global cyber threat landscape, the SCO's strategic importance as a major regional actor, and the potential implications of its cyber security cooperation (or lack thereof) for regional and international stability. The research explores the SCO's evolution as a security actor, the nature of cyber threats facing its members, and critically assesses the organization's specific role, initiatives, and mechanisms in the cyber security domain. Employing a qualitative methodology, the study analyzes official SCO documents, member state policies, expert reports, and secondary academic literature. The paper is structured into three sections: the emergence of the SCO, cyber threats within member states, and the organization's role in cyber security. This approach provides a comprehensive overview and critical evaluation of the SCO's response to a critical 21st-century security challenge.

Keywords: Shanghai Cooperation Organization (SCO), cyber security, Cyber Threats, Regionalism, Security Community, International Relations, Regional Security, Cooperation.

التعاون في مجال الأمن السيبراني في إطار منظمة شنغهاي للتعاون

د. أحمد محمد صلاح الدين الألفي

مدرس القانون الدولي العام بكلية الحقوق جامعة بني سويف

الملخص:

يشهد النظام الدولي المعاصر تحولًا عميقًا، حيث أدت العولمة والتطور التكنولوجي المتسارع إلى زيادة الترابط بين الدول، مما أتاح فرصًا للتعاون لمواجهة التحديات المشتركة، ولكنه في الوقت ذاته خلق نقاط ضعف جديدة وهددات عابرة للحدود. في هذا السياق، تكتسب مفاهيم مثل "المجتمعات الأمنية" و"الإقليمية" أهمية متزايدة، حيث تسعى

الدول إلى بناء علاقات مستقرة وتعاون إقليمي لمواجهة التحديات المشتركة وتعزيز الاستقرار. تمثل منظمة شنغهاي للتعاون (SCO) نموذجًا بارزًا لهذه التوجهات الإقليمية في أوراسيا، حيث تطورت من آلية لتسوية النزاعات الحدودية إلى منظمة متعددة الأغراض تشمل الأبعاد السياسية والاقتصادية والأمنية.

تواجه الدول الأعضاء في منظمة شنغهاي للتعاون تحديات أمنية متزايدة، تبرز من بينها التهديدات السيبرانية، بما في ذلك الإرهاب السيبراني، مما يستلزم جهدًا تعاونيًا كبيرًا للتصدي لها. على الرغم من الأهمية المتزايدة لهذه التهديدات والدور الأمني الواسع للمنظمة الذي حظي باهتمام بحثي، لا تزال هناك فجوة معرفية فيما يتعلق بتحليل آليات وفعالية وقيود التعاون المحدد داخل إطار المنظمة في مجال الأمن السيبراني.

تهدف هذه الدراسة إلى سد هذه الفجوة من خلال تقديم تحليل معمق لانخراط منظمة شنغهاي للتعاون في قضايا الأمن السيبراني. تكمن أهمية البحث في تصاعد التهديدات السيبرانية عالميًا، والمكانة الاستراتيجية للمنظمة، وتأثير تعاونها (أو غيابه) على الاستقرار الإقليمي والدولي. تسعى الدراسة للإجابة على أسئلة بحثية حول نشأة المنظمة، وطبيعة التهديدات السيبرانية التي تواجه أعضائها، والدور الذي تلعبه المنظمة، بما في ذلك مبادراتها وآلياتها وفعاليتها في مجال الأمن السيبراني. يعتمد البحث على منهجية تحليل نوعي للوثائق الرسمية للمنظمة، والسياسات الوطنية للدول الأعضاء، وتقارير الجهات المتخصصة، والأدبيات الأكاديمية الثانوية. يتكون البحث من ثلاثة أقسام: نشأة المنظمة، التهديدات السيبرانية داخل الدول الأعضاء، ودور المنظمة في مجال الأمن السيبراني.

الكلمات المفتاحية : منظمة شنغهاي للتعاون، الأمن السيبراني، التهديدات السيبرانية، الإقليمية، المجتمع الأمني، العلاقات الدولية، الأمن الإقليمي، التعاون.

(ISSN: 2537 - 0758)

Introduction:

The contemporary international system is in a perpetual state of flux, undergoing a profound transformation characterized by the pervasive influence of globalization. This multifaceted phenomenon, propelled by enhanced interconnectedness via advancements in transportation, communication, and information technology, ostensibly fosters a global community ostensibly poised to address shared challenges. However, the putative benefits of globalization are often juxtaposed with tangible drawbacks, as geopolitical tensions increasingly transcend localized boundaries, impacting regional and global stability. The complex interdependence of global trade, economic ties, and interconnected capital markets creates a reciprocal dynamic that significantly influences political and economic processes across diverse regions.

Within this dynamic landscape, regionalization has emerged as a demonstrably crucial trend, with states actively striving to establish stable relations with neighboring countries to enhance their respective potential and address pressing, localized regional issues. This concerted effort has led to the emergence of diverse forms of cooperation, ranging from traditional regional integration models to more flexible and context-specific approaches tailored to address particularized needs and geopolitical goals. Security communities, driven by the fundamental concept of collective cooperation, ostensibly play a vital role in establishing political stability by fostering revised interpretations of social reality, thereby incentivizing collaborative action among both state and non-state actors.

Against this complex backdrop, the Shanghai Cooperation Organization (SCO) stands as a particularly significant regional entity grappling with a multitude of contemporary security challenges, most notably the pervasive and evolving threat of cyber terrorism. This transnational threat inherently transcends national borders, thus necessitating concerted efforts from member states to effectively mitigate its potentially devastating impact. Documented instances of targeted cyber attacks impacting SCO member states,

including India, the Russian Federation, and Pakistan, underscore the manifest urgency of addressing this critical issue. Recognizing the inherently transnational nature of cybercrime, the SCO has undertaken preliminary steps aimed at fostering multilateral joint efforts and promoting broad-based international cooperation within the cyber security domain. This research endeavor seeks to provide a rigorous and critical analysis of the SCO's efforts in combating cyber terrorism, examining its organizational structure, strategic initiatives, and the overall effectiveness of its multifaceted approach in addressing this increasingly salient and complex threat".

Research Objectives:

• Primary Objective: To critically evaluate the efficacy of the Shanghai Cooperation Organization's initiatives in addressing the multifaceted threat of cyber terrorism.

•Secondary Objectives :To delineate the historical context and the multifaceted evolution of the Shanghai Cooperation Organization as a prominent regional actor.

Research Methodology:

This research will adopt a rigorous mixed-methods approach, systematically integrating both qualitative and quantitative data to facilitate a comprehensive and nuanced analysis of the SCO's complex role in combating cyber terrorism. The study will employ the following methodological

• Content Analysis: A systematic examination of official documents promulgated by the Shanghai Cooperation Organization, security intelligence reports, and peer-reviewed academic studies pertaining to cyber terrorism.

(ISSN: 2537 - 0758)

•Case Study Analysis: An in-depth analysis of selected cases of cyber-attacks targeting SCO member states, meticulously analyzing the SCO's responses and their effectiveness.

• Comparative Analysis: A structured comparison of the SCO's strategic approach with the strategies employed by other regional and international organizations in the domain of cyber terrorism mitigation.

Significance of the Study:

This research endeavor possesses significant scholarly and practical import for several compelling reasons:

• Clarifying the SCO's Role: It contributes substantively to a more refined understanding of the Shanghai Cooperation Organization's complex role in confronting contemporary security threats, with a particular emphasis on the multifaceted challenge of cyber terrorism.

• Providing Strategic Insights: The research will offer strategically relevant insights for policymakers, academic researchers, and security professionals regarding effective approaches to fostering regional and international cooperation in the domain of cyber terrorism mitigation and prevention.

- Informing Policy Development: The findings and recommendations derived from this study can demonstrably contribute to the development and implementation of more robust and effective policies and strategies for combating cyber terrorism at the national, regional, and global levels.

Research Structure:

The research will be structured into the following chapters:

Section One: The Emergence of the Shanghai Cooperation Organization.

Section Two: Cyber Threats within the Organization's Member States.

Section three: The Role and Efforts of the Shanghai Cooperation Organization in Cyber security.

Section One: The Emergence of the Shanghai Cooperation Organization

1.1 The Organization's Charter

The Shanghai Cooperation Organization (SCO) is a permanent regional intergovernmental organization founded in Shanghai on June 15, 2001, by its initial member states. Its Charter entered into force on September 19, 2003. According to the Charter, the SCO aims to strengthen mutual trust, friendship, and good-neighborliness among member states; enhance multilateral cooperation in maintaining and strengthening regional peace, security, and stability; jointly address new challenges and threats; encourage effective and mutually beneficial cooperation in various fields; and contribute to the economic, social, and cultural development of its members. The organization is founded on principles including mutual respect for sovereignty, independence, territorial integrity, the inviolability of state borders, non-interference in internal affairs, non-use or threat of force, and equality among all member states[1].

Since 2005, the SCO has held observer status in the UN General Assembly. In April 2010, the UN and SCO Secretariats signed a Joint Declaration on Cooperation. The SCO Secretariat has also established partnerships with UNESCO, the World Tourism Organization (UNWTO), and the International Organization for Migration (IOM), alongside ongoing cooperation with the UN Office on Drugs and Crime (UNODC), the UN Economic and Social Commission for Asia and the Pacific (ESCAP), and the UN Office of Counter-Terrorism (UNOCT). The UN Department of Political and Peacebuilding Affairs (DPPA) and the UN Regional Centre for Preventive Diplomacy for Central Asia (UNRCCA) maintain regular contact with SCO officials, focusing on regional

[1] The Shanghai Cooperation Organization, http://eng.sectsco.org/about_sco /, Accessed on: 29/9/2024

(ISSN: 2537 - 0758)

security developments and key issues related to counter-terrorism and preventing violent extremism.

SCO Member States affirm their determination to intensify cooperation against terrorism, separatism, and extremism—transnational threats they believe can only be effectively addressed through the collective efforts of the international community. They categorically reject all acts and methods of terrorism. Furthermore, SCO Member States advocate for establishing a global network to counter new threats and challenges, emphasizing the central coordinating role of the United Nations and its Security Council. Such a network would ideally involve multilateral cooperation on early warning, prevention, and resolute responses to emerging threats[2].

1.2 Organizational Structure

The SCO's main bodies include the Council of Heads of State, the Council of Heads of Government (Prime Ministers), the Council of Ministers of Foreign Affairs, Meetings of Heads of Other Ministries and/or Agencies, and the Council of National Coordinators.

- The Council of Heads of State: This is the supreme decision-making body, convening annually at summits held in one of the member states' capitals. It comprises the Presidents or highest-ranking leaders of the member states.
- The Council of Heads of Government (Prime Ministers): This is the second-highest body, holding annual summits to discuss cooperation issues and approve the organization's budget. It comprises the Prime Ministers or equivalent heads of government of the member states. *(For example, as of recent years, this would include individuals like Li Keqiang representing China or Narendra Modi*

[2] Russian Federation. Permanent Representative to the United Nations. (2002, June 14). *Letter addressed to the Secretary-General*. United Nations. pp. 3-5

representing India, though specific officeholders change over time).

- The Council of Foreign Ministers: Holds regular meetings to discuss the international situation and the SCO's external relations.
- The Council of National Coordinators: Manages and coordinates the day-to-day activities and interactions within the SCO framework[3].

The SCO has two permanent bodies:

- The SCO Secretariat: Headquartered in Beijing, China, established in 2004. It provides administrative, technical, and informational support.
- The Executive Committee of the Regional Anti-Terrorism Structure (RATS): Headquartered in Tashkent, Uzbekistan, also formally announced in 2004[4].

The establishment and continuous operation of these two permanent bodies marked the completion of the SCO's initial formation phase and its transition into comprehensive operational cooperation.

The Regional Anti-Terrorism Structure (RATS) is a key permanent organ dedicated to enhancing cooperation among member states against the "three evils" of terrorism, separatism, and extremism. The Director of the RATS Executive Committee is elected for a three-year term. Each member state also appoints a permanent representative to RATS[5].

[3] Session of the Council of Foreign Ministers from Member States of the Shanghai Cooperation Organization " (Press release). Kuala Lumpur: Embassy of the Russian Federation in Malaysia. 9-07-2007.

[4] The Shanghai cooperation organization , available at : https:// eng . sectsco . org/aboutsco / accessed on: 30-9-2024

[5] Information on Regional Anti-Terrorist Structure of Shanghai Cooperation Organization .

(ISSN: 2537 - 0758)

1.3 Scope of the Organization's Mandate

The SCO aims to establish a legal and regulatory basis for cooperation among its members in international information security. This includes coordinating and implementing joint measures to ensure security in the information space, potentially establishing systems for monitoring and responding to threats, and contributing to the development of international legal norms concerning information weapons that could threaten defense capabilities, national security, or public safety.

The SCO Charter reiterates core principles of international law such as non-aggression and non-interference in internal affairs. While specific treaty language should be consulted, the broader security goals often relate to fostering a stable regional environment[6].

Membership in the SCO is open to states in the region that meet the criteria outlined in its legal documents and receive the consensus approval of existing members. While initially focused on Central Asia, the organization has expanded significantly (e.g., including India, Pakistan, and Iran), demonstrating that the relevant "region" is interpreted broadly, encompassing states willing to adhere to the SCO's objectives, particularly concerning regional security threats[7].

The SCO has identified primary threats to international information security, including: the development and use of information as a weapon (information warfare), information terrorism, cybercrime, and the dissemination of information intended to harm the socio-political and economic stability of other states. In defining these threats, its approach shares some similarities with frameworks like the Arab Convention on Combating Information Technology Offences, although specific comparisons require detailed analysis

[6] Charter of the Organization, Article 2.1:
https:// www. Sectsco.org/EN123/show. asp? id Accessed on: 9/30/2024.

[7] Mutlaq Al- Qahtanti (20 March 2006). The Shanghai cooperation organization and the Law of international organizations . Oxford University Press.

of the relevant SCO agreements (such as the Agreement on Cooperation in the Field of International Information Security).

The establishment of the RATS Executive Committee in Tashkent in 2005 reflected the SCO's commitment to operationalizing its counter-terrorism goals, as outlined in the Charter and the foundational Shanghai Convention on Combating Terrorism, Separatism and Extremism. The choice of Tashkent is often seen as reflecting Uzbekistan's regional significance and commitment to counter-terrorism efforts.

The key tasks and duties of the RATS Executive Committee include:

1. Maintaining working relations with relevant member state institutions and international organizations on counter-terrorism issues.
2. Assisting member states in preparing and conducting joint counter-terrorism exercises.
3. Drafting joint proposals for international legal documents related to combating terrorism, separatism, and extremism.
4. Collecting and analyzing relevant information received from member states.
5. Contributing to effective responses to global challenges and threats within its mandate.
6. Organizing scientific conferences and workshops, and facilitating the exchange of expertise in combating terrorism, separatism, and extremism.

Section Two: Cyber Threats within the Organization's Member States

Several member states of the Shanghai Cooperation Organisation (SCO) have experienced significant cyberattacks, resulting in considerable consequences. The recurring nature of these incidents

(ISSN: 2537 - 0758)

underscores the persistent cybersecurity challenges faced by SCO members. This document examines notable cyber incidents affecting key member states, specifically India, Russia, and Pakistan.

India

India has been a frequent target of malicious cyber activities. Significant incidents include:

1. Compromise of Government Email Accounts (June 2012): Over 10,000 email addresses belonging to senior Indian government officials were reportedly compromised on June 12, 2012. Described at the time as one of the largest cyberattacks targeting the nation's official networks, the incident affected personnel within the Prime Minister's Office, the Ministries of Defence, External Affairs, Home Affairs, and Finance, as well as intelligence agencies. Indian officials attributed the attack to state-sponsored actors perceived as hostile to India's national interests. This information was corroborated by officials from intelligence and law enforcement agencies during a conference held by the National Critical Information Infrastructure Protection Centre (NCIIPC) in New Delhi. An official from the National Technical Research Organisation (NTRO) acknowledged the incident without identifying the specific perpetrators, stating that destructive and disruptive processes were initiated and that countermeasures were deployed[8].
2. Lazarus Group Activities (2018-2019):
    - Financial Sector Espionage (September 2019): Cybersecurity firm Kaspersky Lab reported the presence of malware actively targeting several Indian financial institutions and research centers.

[8] Ajmer Singh (Dec 18 2012) Over 10,000 email IDs hit in 'worst' cyber attack, The Indian Express, http://archive.indianexpress.com/news/over-10000-email-ids-hit-in- worst-cyber-attack/1046874, accessed on:1/10/2024.

Kaspersky researchers attributed the malware, designed for data exfiltration (uploading/downloading files from compromised systems), to the Lazarus cyber-espionage group, which has been linked to previous attacks against Indian targets.

- ATM Malware (2018): Kaspersky researchers identified malware designated "ATMDtrack," specifically engineered to infiltrate Indian Automated Teller Machines (ATMs) and steal customer card data. Subsequently, over 180 related malware variants were discovered, though these samples did not appear to target ATMs directly[9].

3. Kudankulam Nuclear Power Plant Breach (November 2019): India's largest nuclear power facility, the Kudankulam Nuclear Power Plant, was reportedly breached by actors linked to North Korea, following India's advancements in thorium-based reactor research. While the potential for causing physical damage existed, the attackers' primary objective appeared to be data exfiltration. According to Indian government sources, the attack, suspected to involve the Lazarus group (often associated with North Korean state operations), aimed to gather intelligence on India's thorium technology development programme[10].

[9] Malware found targeting Indian financial institutions (Sep 23, 2019), ATM: Kaspersky, Times of India, https://timesofindia.indiatimes.com/business/india-business/malware-found-targeting-indian-financial-institutions-atm-kaspersky/articleshow/71264729.cms accessed on: 5/10/2024

[10] Prabhjote Gill (13 November 2019), Here's why North Korean hackers attacked India's nuclear power plant, Business Insider, https://www.businessinsider.in/tech/news/indian-nuclear-plant-hack-is-only-one-small-part-of-a-much-bigger-operation-according-to-a-cybersecurity-expert/articleshow/72033253.cms accessed on:5/10/2024

(ISSN: 2537 - 0758)

4. COVID-19 Themed Phishing Campaign (June 2020): India was identified as one of six countries potentially targeted by a North Korean phishing campaign leveraging the COVID-19 pandemic. Attributed to the Lazarus group, this campaign targeted individuals and businesses across India, Singapore, South Korea, the United Kingdom, and the United States. The apparent motive was financial gain, achieved by luring email recipients to fraudulent websites designed to harvest personal and financial information. In response, India's Computer Emergency Response Team (CERT-In) issued an advisory warning of potential phishing attacks impersonating government agencies or other entities involved in disbursing COVID-19 financial aid or offering free testing services[11].

Russia

Russia has also faced sophisticated cyber threats, including:

1. Lazarus Group Targeting Russian Entities (2019)[12]: In what was described as an unusual development, the Lazarus group, specifically its subunit Blueboroff (known primarily for global espionage campaigns), reportedly conducted coordinated attacks against Russian-based companies over several weeks in 2019. Typically, Lazarus group activities align with geopolitical tensions involving North Korea and the United States, Japan, or South Korea. The targeting of Russian organizations represented a deviation from this pattern. Attack methodologies involved using documents with embedded malicious code, employing luring images to

[11] ANS (20 June 2020) North Korean Hackers May Target India on June 21 With COVID-19 Phishing Emails, India.com, https://www.india.com/technology/north- korean-hackers-may-target-india-on-june-21-with-covid-19-phishing-emails- 4063343/, accessed on: 5/10/2024

[12] Ms. Smith (FEB 20, 2019), North Korean hackers target Russian-based companies, CSO, https://www.csoonline.com/article/3341799/north-korean-hackers-target- russian-based-companies.html, accessed on: 6/10/2024.

convince victims to enable macros ("Enable Content"), thereby executing the malware[13].

2. Yandex Network Intrusion (October-November 2018): The Russian internet company Yandex experienced a network intrusion between October and November 2018. The attackers, suspected to be state-sponsored actors working for foreign intelligence agencies, deployed malware in an attempt to spy on user accounts. Sources indicated difficulty in definitively attributing the attack to a specific state actor. A Yandex spokesperson stated that the company's security team detected the attack early and neutralized it before any user data was compromised. The attackers' objective appeared to be acquiring technical information regarding Yandex's user account authentication processes, which could potentially enable intelligence agencies to impersonate users and access private communications. Kremlin spokesman Dmitry Peskov commented that the Russian government was unaware of this specific incident but acknowledged that Yandex and other Russian companies face frequent cyber-attacks, many originating from foreign countries[14].

[13] North Korea Turns Against New Targets. (February 19, 2019), Check Point Research, https://research.checkpoint.com/2019/north-korea-turns-against-russian- targets ،
accessed on:6/10/2024.

[14] Christopher Bing, Jack Stubbs, Joseph Menn (June 27, 2019), Exclusive: Western intelligence hacked 'Russia's Google' Yandex to spy on accounts - sources, Reuters, https://www.reuters.com/article/us-usa-cyber-yandex-exclusive/exclusive-western- intelligence-hacked-russias-google-yandex-to-spy-on-accounts-sources- idUSKCN1TS25X ،
Accessed on: 6/10/2024.

(ISSN: 2537 - 0758)

Pakistan

Pakistan has been subjected to various cyber espionage and intrusion campaigns:

1. **Cyber Espionage Targeting Indian and Pakistani Entities (October 2016):**

   A cyber security firm reported on a cyber-espionage campaign targeting entities in both India and Pakistan. While potentially involving multiple threat actors, the Tactics, Techniques, and Procedures (TTPs) suggested shared objectives or sponsorship, likely by a nation-state. The campaign potentially targeted government and military organizations with interests in South Asian regional security. Attackers used lure documents themed around South Asian security matters, including reports from news agencies like Reuters and Zee News concerning military affairs and the Kashmir conflict. The malware employed featured capabilities for file upload/exfiltration, secure deletion, command execution, reconnaissance, and data theft, utilising backdoor access techniques. The campaign also involved variants targeting Android mobile devices[15].

2. **Targeting of Government Officials via WhatsApp Vulnerability (2019):**

   In 2019, the mobile devices of at least two dozen Pakistani government officials, including senior defence and intelligence personnel, were reportedly targeted using spyware technology developed by the Israeli firm NSO Group. These attacks exploited a known vulnerability in the WhatsApp messaging application, potentially allowing attackers to access messages and other data on the targeted phones. While Pakistan has not publicly confirmed the incident, government actions suggest

[15] Rahul Bhatia (28 August 2017), Exclusive: India and Pakistan hit by spy malware- cyber security firm, Reuters, https://www.reuters.com/article/us-india-cyber-threat/exclusive-india-and-pakistan-hit-by-spy-malware-cybersecurity-firm- idUSKCN1B80Y2
accessed on: 6/10/2024.

acknowledgement of the threat. Arslan Khalid, then a senior advisor on digital matters to Prime Minister Imran Khan, indicated the government was developing a secure alternative to WhatsApp for sensitive communications. Officials at Pakistan's Ministry of Information Technology reportedly advised government personnel to cease using WhatsApp for confidential information and to replace smartphones acquired before May 2019[16].

3. Targeting of Telecommunications Sector by Iranian Actors (Reported May 2020)[17]:

Cybersecurity firm Symantec reported that an Iranian hacking group known as "Greenbug" (or Seedworm/APT34) had been targeting IT infrastructure across South Asia for several months. The campaign specifically compromised at least three telecommunications companies in Pakistan, gaining access to their data servers. Symantec's report detailed the group's methods, including the use of tunneling techniques (like VPNs or proxies) to maintain persistent, low-observable access to compromised networks, facilitating lateral movement and data exfiltration. While the specific companies were not named, the report highlighted the persistence of such threat actors. John DiMaggio, a senior cyber threat analyst at Symantec, commented on the group's tenacity, stating, "When we close one door, they will try to come back through the other,"

[16] Stephanie Kirchgaessner (19 December 2019), Israeli spyware allegedly used to target Pakistani officials' phones, The Guardian,, https://www.theguardian.com/world/2019/dec/19/israeli-spyware-allegedly-used- to-target-Pakistani-officials-phones ،Accessed on: 7/10/2024.

[17] Aasil Ahmed (May 2020), 3 Major Pakistani Telecom Companies Have Been Attacked by Iranian Hackers, Pro Pakistani,, https://propakistani.pk/2020/05/20/3-major-pakistani-telecom-companies-have-been-attacked-by-iranianhackers/#:~:text=A%20group%20of%20Irani an%20hackers, servers%20when%20it%2 Osuits%20them, accessed on: 7/10/2024.

(ISSN: 2537 - 0758)

emphasizing the ongoing challenge in defending against determined adversaries[18].

Section three: The Role and Efforts of the Shanghai Cooperation Organization in Cyber security

In response to the significant and recurring cyber threats faced by its member states, the Shanghai Cooperation Organization (SCO) and its constituent nations have undertaken various measures to address this challenge. This section outlines the efforts initiated by SCO member states, both individually and collectively through the Organization, in the domain of cyber security, and considers the international context of these initiatives.

1.1 Cyber security Efforts within the SCO Framework

Initial Bilateral and National Initiatives:

Prior to extensive collective action, individual SCO member states initiated steps towards enhancing cyber security. For instance, the Ministry of Communications and Information Technology, Government of India, established cooperative frameworks through Memoranda of Understanding (MoUs) and other agreements focused on development and information sharing with various countries. Notably, India and South Korea signed a joint statement in 2004 fostering bilateral cooperation in information technology. Furthermore, the Indian Computer Emergency Response Team (CERT-In) executed an MoU with the Korea Internet & Security Agency (KISA) to formalize cooperation specifically in cyber security[19].

[18] Sean Lyngaas (19 May 2020), 'Greenbug' hacking group hits three telecom firms in Pakistan, Cyberscoop, https://www.cyberscoop.com/greenbug-symantec-iran- hacking-pakistan/ accessed on: 7/10/2024.

[19] Touré, Hamdoun. (2011, January). The Search for Cyber Peace. International Telecommunication Union.

Collective SCO Approach and Foundational Documents: The SCO, as an entity, conceptualizes 'international information security' (IIS) not only in terms of infrastructure protection but also with a perspective that internet content can pose potential security threats requiring regulation. Consequently, the Organization has pursued numerous initiatives aimed at mitigating these perceived threats.

- Action Plan (2007): Recognizing the emerging challenges in information security, the SCO Council of Heads of State, during its seventh meeting in Bishkek (August 2007 - *Note: Original text says 2007, location implied*), saw the signing of the "Action Plan of the SCO Member States for Ensuring International Information Security" by China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, and Uzbekistan. This document formalized cooperation to jointly address threats to network and information security[20].

Key Declarations and Ongoing Cooperation:

SCO member states have consistently utilized high-level declarations to articulate their concerns and commitments regarding IIS. Common themes include the potential misuse of Information and Communication Technologies (ICTs) contrary to international stability and security objectives, the necessity for continued cooperation in IIS, and the recognition that transnational cybercrime demands broad international collaboration. This commitment is reflected in successive summit declarations:

- Dushanbe Declaration (August 2008): The SCO Council of Heads of State meeting in Dushanbe issued a joint statement emphasizing concerns about the potential use of modern ICTs for purposes conflicting with international stability and security. It acknowledged the SCO's ongoing efforts in developing international legal frameworks and practical

[20] The Shanghai Cooperation Organization (SCO), Cybercrime law, https://www.cybercrimelaw.net/SCO.html, accessed on:14/10/2024

(ISSN: 2537 - 0758)

cooperation mechanisms for IIS. The declaration stressed respect for national traditions, state sovereignty, territorial integrity, and good neighbourliness. It also noted the importance of UN General Assembly Resolution 62/17 ("Developments in the field of information and telecommunications in the context of international security") and expressed members' readiness to promote its implementation[21].

- Yekaterinburg Declaration (June 2009): Meeting in Yekaterinburg, Russia, the SCO Heads of State reaffirmed the significance of ensuring IIS as a critical component of the overall international security architecture. The declaration underscored the need to strengthen the legal foundations of international relations based on generally accepted principles of international law and state obligations. It highlighted the task of enhancing the UN's coordinating role and strengthening mechanisms for responding to global challenges. Member states expressed intent to coordinate on UN reform, including Security Council reform. Crucially, the declaration reiterated that maintaining international peace requires conditions of equal security for all states, advocating for political and diplomatic resolution of conflicts without interference in internal affairs, based on the principle that the security of one state should not be pursued at the expense of another's[22].
- Tashkent Declaration (June 2010): The 10th meeting of the SCO Council of Heads of State in Tashkent involved extensive discussions on global and regional issues. The resulting declaration reaffirmed commitment to close cooperation within the SCO to enhance its role in regional and global security and stability. It included commitments to enhance counter-terrorism cooperation, including with observer states and relevant regional bodies. Specific to

[21] Dushanbe Declaration, SCO, http://eng.sectsco.org. P p: 1, 2.
[22] Yekaterinburg Declaratio, SCO, http://eng.sectsco.org, pp: 1, 2.

cyber threats, Member States agreed on the necessity of continued cooperation in IIS and resolved to accelerate the implementation of the intergovernmental *Agreement on Cooperation in Ensuring International Information Security* (signed in Yekaterinburg, 2009). Cooperation in securing major joint events was also commended.

- Astana Declaration (June 2011) : Marking the SCO's 10th anniversary in Astana, Kazakhstan, the Heads of State emphasized the solid foundation built for safeguarding security and stability. The declaration highlighted intentions to promote major projects (transport, communications, innovative technologies) and establish financing mechanisms, viewing these as contributing to trade, regional development, and Asia-Europe connectivity. It reiterated significant concern regarding threats arising from the misuse of ICTs and stated that transnational cybercrime necessitates joint efforts and broad international cooperation. The declaration affirmed that security, economic cooperation, and population well-being remain long-term SCO priorities, emphasizing cooperation based on trust, respect for cultural diversity, and joint goal implementation[23].
- Beijing Declaration (June 2012): The SCO Council of Heads of State meeting in Beijing acknowledged the Organisation's positive impact on regional cooperation, good neighbourliness, and mutual trust. Key documents approved included revised regulations on political and diplomatic measures and response mechanisms for threats to peace and stability, alongside a cooperation program for counter-terrorism (2013-2015). The Heads of State again stressed the importance of cooperation in protecting IIS and preventing the use of ICTs to undermine peace and security. They also highlighted the importance of cooperation in

[23] Astana Declaration, SCO, http://eng.sectsco.org. pp:1,4,5.

(ISSN: 2537 - 0758)

cultural, scientific, technological, tourism, and health sectors, including sanitation and epidemic control[24].

Practical Implementation: Conferences and Exercises

Beyond declarations, the SCO has engaged in practical activities:

- China Information Security Conference: Platforms like the "China Information Security Conference" (various iterations, e.g., the 10th focusing on "Trust and Security in the Digital Future") serve as forums for exchanging views on combating cybercrime, emerging technologies (like 5G), internet governance, and building a secure information space. Discussions encompass risk assessment, international cooperation in digital transformation, e-commerce, smart cities, and AI. SCO Secretary-General Vladimir Norov, in messages to such events, has reiterated that IIS, combating cyberterrorism and cybercrime, and preventing the spread of extremist ideologies via ICT networks are SCO priorities. He highlighted the practical work of the SCO's Regional Anti-Terrorist Structure (RCTS) in identifying, preventing, and disrupting terrorist/extremist activities online, including countering propaganda. RCTS efforts reportedly led to restricted access to over 165,000 online resources and the disruption of activities of 3,000 individuals associated with online extremist groups in 2018 alone. Mr. Norov emphasized the SCO's commitment to a peaceful, secure, and cooperative information space, noting that the SCO Development Strategy Towards 2025 prioritizes IIS, effective internet oversight, and mechanisms to counter the

[24] Press Communiqué of the Meeting of the Council of The Heads of the Member States of The Shanghai Cooperation Organization (,7 June2012) Ministry of Foreign of Affairs of the People's Republic of China,https://www.fmprc.gov.cn/mfa eng/wjdt 665385/2649 665393/t939161.shtml. Accessed on: 15/10/2024.

use of ICTs for terrorist purposes and other threats to member states' security.

- Joint Cyber Counter-Terrorism Exercises: The SCO has conducted joint exercises focused specifically on cyber aspects of counter-terrorism:
    - October 27, 2015 (Xiamen, China): First online counter-terrorism exercise focused on exchanging law enforcement techniques and technical capabilities[25].
    - December 2017 (Xiamen, China): First joint *cyber* counter-terrorism drills, aimed at enhancing trust and cooperation (as noted by China's then-Vice Minister of Public Security, Xi Jun)[26].
    - December 2019 (Xiamen, China): Joint online counter-terrorism exercise simulating a response to an international terrorist organization disseminating illicit information online, reflecting the growing challenge of cyber threats in this domain.

[25] SCO countries hold drill targeting cyber-terrorism (6 December, 2017), Xinhua, http://www.xinhuanet.com/english/2017-12/06/c 136806108.htm accessed on: 15/11/2024.

[26] SCO carries out online anti-terrorism drill (12 December 2019, Global Times, https://www.globaltimes.cn/content/1173369.shtml, accessed on: 15/11/2024.

(ISSN: 2537 - 0758)

References

I. Articles, Books, and Research Papers

1. Ahmed, Aasil. (2020, May 20). 3 Major Pakistani Telecom Companies Have Been Attacked by Iranian Hackers. *ProPakistani*. Retrieved October 7, 2024, from https://propakistani.pk/2020/05/20/3-major-pakistani-telecom-companies-have-been-attacked-by-iranian-hackers/
2. Al-Issawi, Muhammad Hussein Kazim. (2015). The Shanghai Cooperation Organization within the Framework of International Law. *Journal of Legal Sciences* (Baghdad), [Volume/Issue if known], 34-35.
3. Al-Qahtani, Mutlaq. (2006). *The Shanghai Cooperation Organization and the Law of International Organizations*. Oxford University Press.
4. ANS. (2020, June 20). North Korean Hackers May Target India on June 21 With COVID-19 Phishing Emails. *India.com*. Retrieved October 5, 2024, from https://www.india.com/technology/north-korean-hackers-may-target-india-on-june-21-with-covid-19-phishing-emails-4063343/
5. Bhatia, Rahul. (2017, August 28). Exclusive: India and Pakistan hit by spy malware - cybersecurity firm. *Reuters*. Retrieved October 6, 2024, from https://www.reuters.com/article/us-india-cyber-threat/exclusive-india-and-pakistan-hit-by-spy-malware-cybersecurity-firm-idUSKCN1B80Y2
6. Bing, Christopher, Stubbs, Jack, & Menn, Joseph. (2019, June 27). Exclusive: Western intelligence hacked 'Russia's Google' Yandex to spy on accounts - sources. *Reuters*. Retrieved October 6, 2024, from https://www.reuters.com/article/us-usa-cyber-yandex-exclusive/exclusive-western-intelligence-hacked-russias-google-yandex-to-spy-on-accounts-sources-idUSKCN1TS25X
7. Gill, Prabhjote. (2019, November 13). Here's why North Korean hackers attacked India's nuclear power plant. *Business Insider India*. Retrieved October 5, 2024, from https://www.businessinsider.in/tech/news/indian-nuclear-

plant-hack-is-only-one-small-part-of-a-much-bigger-operation-according-to-a-cybersecurity-expert/articleshow/72033253.cms

8. Kirchgaessner, Stephanie. (2019, December 19). Israeli spyware allegedly used to target Pakistani officials' phones. *The Guardian*. Retrieved October 7, 2024, from https://www.theguardian.com/world/2019/dec/19/israeli-spyware-allegedly-used-to-target-pakistani-officials-phones
9. Lyngaas, Sean. (2020, May 19). 'Greenbug' hacking group hits three telecom firms in Pakistan. *Cyberscoop*. Retrieved October 7, 2024, from https://www.cyberscoop.com/greenbug-symantec-iran-hacking-pakistan/
10. Malware found targeting Indian financial institutions, ATM: Kaspersky. (2019, September 23). *Times of India*. Retrieved October 5, 2024, from https://timesofindia.indiatimes.com/business/india-business/malware-found-targeting-indian-financial-institutions-atm-kaspersky/articleshow/71264729.cms
11. SCO carries out online anti-terrorism drill. (2019, December 12). *Global Times*. Retrieved November 16, 2024, from https://www.globaltimes.cn/content/1173369.shtml
12. Singh, Ajmer. (2012, December 18). Over 10,000 email IDs hit in 'worst' cyber attack. *The Indian Express*. Retrieved October 1, 2024, from http://archive.indianexpress.com/news/over-10000-email-ids-hit-in-worst-cyber-attack/1046874
13. Smith, M. (2019, February 20). North Korean hackers target Russian-based companies. *CSO Online*. Retrieved October 6, 2024, from https://www.csoonline.com/article/3341799/north-korean-hackers-target-russian-based-companies.html
14. Xinhua. (2017, December 6). *SCO countries hold drill targeting cyber-terrorism*. Retrieved November 15, 2024, from http://www.xinhuanet.com/english/2017-12/06/c_136806108.htm

(ISSN: 2537 - 0758)

II. Reports, Websites, and Official Documents:

1. Check Point Research. (2019, February 19). North Korea Turns Against Russian Targets. Check Point Research Blog
2. Cybercrime Law. (n.d.). The Shanghai Cooperation Organization (SCO).
3. Embassy of the Russian Federation in Malaysia. (2007, July 9). Session of the Council of Foreign Ministers from Member States of the Shanghai Cooperation Organization [Press release]. Kuala Lumpur.
4. Ministry of Foreign Affairs of the People's Republic of China. (2012, June 7). Press Communiqué of the Meeting of the Council of the Heads of the Member States of The Shanghai Cooperation Organization.
5. Permanent Representative of the Russian Federation to the United Nations. (2002, June 14). Letter addressed to the Secretary-General. United Nations.
6. Regional Anti-Terrorist Structure of Shanghai Cooperation Organisation. (n.d.). Information on Regional Anti-Terrorist Structure of Shanghai Cooperation Organization.
7. Shanghai Cooperation Organisation. (n.d.). About SCO. Retrieved September 30, 2023, from https://eng.sectsco.org/about_sco/
8. Shanghai Cooperation Organisation. (2002). Charter of the Shanghai Cooperation Organisation.
9. Shanghai Cooperation Organisation. (2008). Dushanbe Declaration. SCO Website., from http://eng.sectsco.org/ [URL likely incomplete - specific path needed.
10. Shanghai Cooperation Organisation. (2009). Yekaterinburg Declaration. SCO Website.
11. Shanghai Cooperation Organisation. (2010). Declaration of the Tenth Meeting of the Council of Heads of Member States of the Shanghai Cooperation Organisation (Tashkent Declaration). SCO Website., from http://eng.sectsco.org/ [URL likely incomplete - specific path needed.[
12. Shanghai Cooperation Organisation. (2011). Astana Declaration on the 10th Anniversary of the Shanghai Cooperation Organisation. SCO Website., from http://eng.sectsco.org/
13. Touré, Hamdoun. (2011, January). The Search for Cyber Peace. International Telecommunication Union.