International Relations and Diplomacy, October 2018, Vol. 6, No. 10, 549-555
doi: 10.17265/2328-2134/2018.10.003

SCO and Cybersecurity: Eastern Security Vision for Cyberspace

Bruna Toso de Alcântara
Federal University of Rio Grande do Sul, Rio Grande do Sul, Brazil

Cyberspace is presenting not only new challenges for states but also new opportunities for power projection. Thus, analyzing how non-Western perspectives have been developed around this subject becomes relevant to understand some dynamics of contemporary international relations. In this way, in order to understand how China and Russia have been behaving in this area, the present paper seeks, through a constructivist approach based on the perspective of the regional complexes, to develop an exploratory research toward the existence of an Eastern regional strategic thinking to cybersecurity, materialized by the Shanghai Cooperation Organization (SCO). To achieve this objective, the paper will use the qualitative document analysis as a method, seeking not only to verify if such Eastern thought for cyberspace is cohesive within the organization, but also to explain what the implications for international society of this thought are.

Keywords: Cyberspace, SCO, Security

Introduction

Established in 2001, and as an evolution of the Shanghai Five Group, the Shanghai Cooperation Organization (SCO) becomes a relevant institution in the Eastern scenario, as it establishes a link between Russia and China, not only with Central Asian countries (i.e., Kazakhstan, Kyrgyzstan, Uzbekistan, and Tajikistan) but also, and more recently, with South Asia, through the incorporation of India and Pakistan.

Therefore, its relevance comes not only from its size, as it comprises about 40% of the world's population and its economic weight, accounting for 20% of world GDP (Harada & Yamada, 2017), but also from its own constitution, which differs from other Western military alliances. This difference emerges since SCO: (1) goes beyond security issues; (2) embraces the cultural and political diversity of its members; (3) operates by consensus; and (4) originated from the necessity over the border and regional affairs management in the post-collapse of the Soviet Union (Bin, 2013).

In this sense, being an organization that congregates independence and interdependence, it is natural that several international issues and threats are perceived in a proper way by the SCO. Moreover, given its geopolitical position, it involves nuclear powers and states with a great international projection into the power table. This ends up shaping much of the SCO orientations, especially towards security, including cyberspace.

Cyberspace gains importance in this context once one considers that critical infrastructures[1], whether

Bruna Toso de Alcântara, Ph.D. candidate in the Postgraduate Program in International Strategic Studies (PPGEEI), Economic Sciences Department, Federal University of Rio Grande do Sul (UFRGS), Rio Grande do Sul, Brazil.

[1] The connection between physical and virtual means occurs through Industrial Control Systems, used in large-scale industrial processes, as is the case of processes that maintain critical infrastructures. In addition, Industrial Control System technologies are often employed in infrastructure industries "to allow a single control center to manage multiple sites" (Shea, 2004, p. 3).

wired or not[2], are attached to it. Thus, cyberspace has a direct impact on the flow of information and the maintenance of these infrastructures, being relevant within SCO scope when considering the energy and transport sectors that interconnect its members. In this way, thinking about cybersecurity and defense is a step towards both the security of national information and the maintenance of SCO itself in its physical or virtual media.

In this sense, this paper seeks to develop an exploratory research toward the existence of an Eastern regional strategic thinking to cybersecurity, materialized by the SCO. To achieve this objective, the paper will use a constructive approach based on the perspective of the regional complexes (Buzan & Weaver, 2003). Additionally, it will use as a method, the qualitative document analysis, seeking not only to verify if such Eastern thought for cyberspace is cohesive within the organization but also to explain what implications for international society of this thought.

Geopolitics of Central Asia and SCO

Based on the assumptions that a region if formed beyond geographical boundaries—being constructed through interdependence and its interactive recognition both internally and externally (Algappa, 2003, p. 25) and that security matters come from speech acts, that is, the idea of threats arises through a social process of securitization—it is feasible to use the concept of Buzan and Waever (2003, p. 44) of Regional Security Complexes (RSC) in the area covered by the SCO: the Asian one. After all, an RSC is "a set of units whose major processes of securitisation, desecuritisation, or both are so interlinked that their security problems cannot reasonably be analysed or resolved apart from one another". In addition, an RSC can be transformed and defined by two types of relationships: the balance of power which gives the tone of the polarity of the system and the pattern of friendship and enmity, generated by a mixture of history, politics, and material conditions (Buzan & Waever, 2003).

In this sense, SCO encompasses both central and southern Asia with its effective members. However, in this paper, we will focus on the central region since it was part of the core of the Organization and its states participated in formal discussions on the cybersecurity in the mid-2000s. Thus, what is important to note in the Central Asian region is a balance of power among China, Russia, and the United States, where the patterns of friendship and enmity involves a former Soviet's power space which, more recently, depends on Chinese material capabilities for its development and at the same time suffers from external security interferences from the United States.

Roughly speaking, the SCO attracts the attention of Russia, China, and the United States given the energy importance of the central Asian region, as well as its natural representation as a bridge between the Middle East and the rest of Asia—facilitating, for example, the displacement of terrorists. Hence, on the one hand, there is a US oscillation towards the region, being more prominent after September 11 and recently, according to Bin (2003), more cooperative with the SCO which seems to give the tone of ideologies and strategic thoughts of the central countries towards the region. And on the other hand, there is an intern dynamic of the Organization materialized by a dual engine encompassing Russia with greater security responsibility and China with greater economic responsibility.

On the Chinese side, the country's influence on the Organization is growing in scope, extrapolating

[2] Wired means refers to those based on fiber optics, telephone cables, and coaxial cables, as well as non-wired and satellite signals and signals that propagate through electromagnetic waves (Fernandes, 2015, p. 607, my translation).

non-security issues and creating a slight Russian animosity in the sense of region control. According to Guang (2013, p. 26), the Chinese influence is projected in the: (1) formulation of theoretical guidelines; (2) the promotion of institutionalization; and (3) the financial support for large projects among the central Asian countries. This movement facilitates the pursuit of national interests for China, including the construction of a stable and secure region for the implementation, for example, of its One Belt One Road project (i.e., new Silk Road), while allowing the country's conduct of a multilateral diplomacy and the development of political, cultural, security, and economic ties with Central Asia. These directives directly influence the heart of friendship or enmity links within the region.

Russia, on its side, does not want to lose its historical influence zone, seeking to soften Chinese influence with initiatives, such as the Customs Union between Russia, Kazakhstan, and Belarus, and the maintenance of Moscow's power over the Eurasian Economic Community (Bin, 2013, p. 49). In addition, the country seeks to maintain its integration plans within the Commonwealth of Independent States (CIS), and therefore, according to Danilovich (2013, p. 34), unlike China, it does not act unconditionally for the development of SCO, taking special care with the presence of other powers in the region.

Thus, this same security mix of influences presents itself in the cyber sector, which in spite serving national objectives, becomes complementary for the construction of a coherent discourse in the area of cybersecurity within the SCO.

Cybersecurity and China

The notion of Chinese cybersecurity differs from the Western one by understanding not only the technical security of networks but also the very content of the Internet, so they prefer in their documents to use the concept of information security (信息安全) rather than cybersecurity. In this sense, according to Lindsay (2015, p. 11), the country has developed a legal and institutional framework more focused on building a censorship and surveillance infrastructure (i.e., the Great Firewall of China) than coordinating technical standards and enforcement mechanisms. In this way, they can better defend against imagined threats, such as terrorism, separatism, and extremism, rather than crime or cyber espionage.

This defensive perception is replicated in the SCO, not only because it allows greater scope for combating the three evils, but also because it fits into the Chinese International Strategy for Cooperation in Cyberspace, of 2017. This strategy foresees as its main objectives:

(1) safeguard sovereignty and security;

(2) develop a system of international rules;

(3) promote fair Internet governance;

(4) protect legitimate rights and interests of citizens;

(5) promote cooperation in the digital economy;

(6) build a platform for cyberculture exchange (China, 2017).

These objectives would be based on 04 principles (i.e., peace, sovereignty, shared governance, and shared benefits) which demonstrate a vision of inequality towards the West, especially the United States, regarding the control of flows of cyberspace (Mckune, 2015, p. 266).

In addition, by allowing a defensive use for "imagined" threats, the country is able to enforce its principle of active defense in cyberspace. This allows greater guarantee of security of national infrastructures and networks, as the National Defense Strategy of 2006 states:

> China pursues a three-step development strategy in modernizing its national defense and armed forces, in accordance with the state's overall plan to realize modernization. The first step is to lay a solid foundation by 2010, the second is to make major progress around 2020, and the third is to basically reach the strategic goal of building informationized armed forces and being capable of winning informationized wars by the mid-21st century. (China, 2006, Section II para 2)

In this sense, it is possible to see Chinese influence in the SCO. The country is using it as a platform to achieve national goals, following a line of thought that merges security with development, and which is replicated within SCO strategies. This replication can be seen through the declaration of Xi Jinping in 2014—during the Group's first meeting Central Security and Computerization of the Internet—when he mentions that "No internet safety means no national security. No informatization means that there is no modernization" (Panda, 2014, para 6).

Cybersecurity and Russia

In a similar way to China, Russia understands cybersecurity as information security. Moreover, Russia's Information Security Doctrine (Доктрина информационной безопасности), created in 2000, is the most relevant document for the Central Asian region, as according to doctrine:

> The state's interests in the information sphere consist of creating conditions for harmonious Russian information infrastructure development and for the exercise of the constitutional rights and freedoms of man and the citizen with respect to receiving and using information to ensure the inviolability of the constitutional system, the sovereignty and territorial integrity of Russia, and political, economic and social stability; the interests of the state also consist of the unconditional maintenance of law and order and in the promotion of equal and mutually advantageous international cooperation. (Rússia, 2000, Section I.1.para 5)

In addition, in a 2013 document entitled "The Basic Principles of the Federative Republic of Russia in the field of Information Security for 2020", there is a need for engagement with the area within the SCO, on a bilateral and multilateral basis of dialogues (Russia, 2013), including advancing the template of the agreement in the area of information security among members (Russia, 2013, p. 5). Objectives that, on the one hand, become tangible in Central Asia due to its dependency on the Russian digital infrastructure, as according to Maness and Valeriano (2015, p. 88), the majority of the Internet, the traffic that comes in and out of the country passes through the Federal Security Service (Federal'naya Sluzhba Bezopasnosti) or by the FSB. On the other hand, these objectives emerge against Chinese interconnection projects in the region.

In this sense, what is observed is that Russia in general, while advocating multilateral dialogue in the cyber field, aims to maintain its security control over the region, reinforcing the idea of the Commonwealth of Independent States and the Security Treaty Organization (CSTO), not only in the basic principles document for 2020, but also in the National Security Strategy for 2020, when it is stated that:

> The development of bilateral and multilateral cooperation with the member states of the Commonwealth of Independent States is a priority direction of Russian foreign policy. Russia will seek to develop the potential for regional and subregional integration and coordination between the CIS Member States, first in the Commonwealth, as well as the CSTO and EvraZEs, which exert a stabilizing influence on the overall situation in the regions on the border with the CIS. (Russia, 2009, p. 5)

Cybersecurity and SCO

The SCO took its ideas of respect to sovereignty, non-interference in the internal affairs of states, equality and mutual respect in the fulfillment of international norms (without double standards) and the fight against the

three evils (i.e., separatism, extremism, and terrorism) to the cyber realm. In fact, it is interesting that in line with Chinese and Russian security visions, the SCO proposes information security as equivalent to what Westerners call cybersecurity, embodied in the Agreement between the Governments of the Member States of the SCO on Cooperation in the Field of Guarantee of International Information Security, signed by China, Russia, Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan.

The Agreement on the Information Security Area was created in 2009, following the repercussion of cyber attacks in Estonia (2007) and during the conflict in Georgia (2008). And, in its second article, it identifies the following threats:

(1) the development and use of weapons of information and preparation to undertake information warfare;

(2) information terrorism;

(3) information crime;

(4) use of dominant position in cyberspace to the detriment of interests and security of other states;

(5) dissemination of information harmful to political systems;

(6) natural and/or human threats to safe and stable operations of the global and national information infrastructure (SCO, 2009, p. 203).

Thus, in addition to the ideas of the SCO embedded in these perceptions, a criticism is made of the Internet governance pattern centered in the United States, since the country has 10 of the 13 root name servers in the world (Pollpeter, 2015, p. 147). Definitions of war and information terrorism—in the annexes to the document—becomes very close to Sino-Russian visions, bearing at the same time the influence of a multilateral approach and mutual trust (SCO, 2009, p. 204). Also, there is the proposition of international engagement in the debates on cybersecurity/information infrastructure (SCO, 2009, p. 204).

This international engagement can already be seen in two moments within the scope of the United Nations. The first was on September 12th , 2011, when four members of the SCO (i.e., China, Russia, Tajikistan, and Uzbekistan) presented a draft International Code of Conduct for Information Security to the United Nations General Assembly (i.e., A66/359), which was rejected. The second moment was in 2015 (i.e., A69/723), when six SCO members, presented a new draft of the code to the UN General Assembly, which was also rejected. This rejection was given based on a perception of excessive state control ideas for cyberspace. However, it is important to highlight that the document also offered an approach of equal rights within a new international law framework, suited (i.e., specific) for the cyber challenges, hence presenting an opposite view of the North Atlantic Treaty Organization (NATO) regarding international law, since NATO advocates for the use of the current developed international law framework, with minor adaptations—proposed in the Tallinn Manual made by the NATO Center for Excellence in Cybernetic Co-operation and Defense (CCDCOE).

Final Considerations

Information security is relevant to SCO members since practical implications in the physical world, especially in the energy and transport infrastructures that interconnect the region, are possible. Likewise, in light of the present paper, it can be said that although there is a clash between two powers in the Asian RSC, covered by the SCO, there is a cohesion of thought and similar international goals. In other words, there is a thought, at least in the hardcore of the Organization, which has a structured cybersecurity project.

Moreover, it is worth emphasizing that there is a difference between the conception of cybersecurity and information security, and that information security is a proposal that seems to rebound the Soviet collective

memory of the need for strong and centralized state control since it is up to the State to secure the content of cyberspace. Therefore, even if this fact could lead to a possible breach of international rights in relation to freedom of expression and privacy, it seems that in the eyes of the East this would be the best way to balance power in cyberspace.

Finally, it is interesting to note that there is a clash of Sino-Russian influences on the Asian region reaching the cyber arena, but in a complementary way. Additionally, they go against the preponderance of the North American power projection in cyberspace at the same time the countries search for already consolidated organizations, such as The United Nations, to propose new models of international legislation in the digital field.

References

Algappa, M. (2003). *Asian security order: Instrumental and normative features*. Stanford: Stanford University Press.

Bin. Y. (2013). The SCO ten years after in search of its own identity. In M. Fredholm (Ed.), *The Shanghai Cooperation Organization and Eurasian geopolitics: New directions, perspectives, and challenges*. Copenhagen: Nordic Institute of Asian Studies (NIAS).

Buzan, B., & Waever, O. (2003). *Regions and powers: The structure of international security*. Cambridge: Cambridge University Press.

China. (2006). *China's national defense in 2006*. Retrieved from https://fas.org/nuke/guide/china/doctrine/wp2006.html#10

China. (2017). *International strategy of cooperation on cyberspace*. Retrieved July 10th, 2017, from http://www.xinhuanet.com/english/china/2017-03/01/c_136094371.htm

Danilovich, M. V. (2013). Approaches to SCO: China and Russia. In A. A. Rozanov (Ed.), *The Shanghai Cooperation Organisation and Central Asian's security challenges* (DCAF Regional Programmes Series No. 16). Geneva: Geneva Centre for Democratic Control of Armed Forces.

Fernandes, J. H. C. (2015). The pernicious cybernetic trap and a proposal for national mobilization. In G. F. Gheller, S. L M. Gonzales, and L. P. Mello (Eds.), *Amazonia and the South Atlantic: Challenges and prospects for defense in Brazil*. Brasília: IPEA.

Guang, P. (2013). The spirit of the Silk Road: The SCO and China's relations with Central Asia. In M. Fredholm (Ed.), *The Shanghai Cooperation Organization and Eurasian geopolitics: New directions, perspectives, and challenges*. Copenhagen: Nordic Institute of Asian Studies (NIAS).

Harada, I., & Yamada, G. (2017) *The SCO welcomes rivals into its fold***.** Retrieved July 10th 2017 from: https://asia.nikkei.com/Economy/The-SCO-welcomes-rivals-into-its-fold2

Lindsay, J. R. (2015). China and cybersecurity: Controversy and context. In J. R. Linsay, T. M. Cheung, and D. Reveron (Eds.), *China and cybersecurity: Espionage, strategy, and politics in the digital domain*. Oxford: Oxford University Press.

Maness, R. C., & Valeriano, B. (2015). *Russia's coercive diplomacy: Energy, cyber, and maritime policy as new sources of power*. New York: Palgrave Macmillan.

Mckune, S. (2015). Foreign hostile forces: The human rights dimension of China's cyber campaigns. In J. R. Linsay, T. M. Cheung, and D. Reveron (Eds.), *China and cybersecurity: Espionage, strategy, and politics in the digital domain*. Oxford: Oxford University Press.

Panda, A. (2014). *Xi Jinping: China should become a 'Cyber Power'*. *The Diplomat*. Retrieved July 10th, 2018, from https://thediplomat.com/2014/03/xi-jinping-china-should-become-a-cyber-power/

Pollpeter, K. (2015). Chinese writings on cyberwarfare and coercion. In J. R. Linsay, T. M. Cheung, and D. Reveron (Eds.), *China and cybersecurity: Espionage, strategy, and politics in the digital domain*. Oxford: Oxford University Press.

Russia. (2000). *Doctrine of information security of the Russian federation*. Retrieved July 10th, 2018, from https://www.itu.int/en/ITU-/Cybersecurity/Documents/National_Strategies_Repository/Russia_2000.pdf

Russia. (2009). *National security strategy of the Russian federation to 2020*. Retrieved July 10th, 2018, from http://mepoforum.sk/wp-content/uploads/2015/08/NDS-RF-2009-en.pdf

Russia. (2013). *Basic principles for state policy of the Russian federation in the field of international information security*. Retrieved July 10th, 2018, from http://www.ccdcoe.org/sites/default/files/strategy/RU_state-policy.pdf

Shanghai Cooperation Organization (SCO). (2009). *Agreement between the governments of state members of the Shanghai Cooperation Organization on cooperation in the field of ensuring the international information security*. Retrieved July 10th, 2018, from http://www.ccdcoe.org/sites/default/files/documents/SCO-090616-IISAgreement.pdf

Shea, D. A. (2004). *Critical infrastructure: Control systems and the terrorist threat*. Retrieved July 10th, 2018, from https://fas.org/irp/crs/RL31534.pdf

United Nations. (2011). *International code of conduct for information security (A66/359)*. Retrieved July 4th, 2018, from https://undocs.org/A/66/359

United Nations. (2015). *International code of conduct for information security (A69/723)*. Retrieved July 4th, 2018, from https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/014/02/PDF/N1501402.pdf?OpenElement