S. RAJARATNAM SCHOOL
OF INTERNATIONAL STUDIES
A Graduate School of Nanyang Technological University

RSIS COMMENTARIES

No. 033/2012 dated 22 February 2012

The Shanghai Cooperation Organisation: Challenges in Cyberspace

By Alica Kizekova

Synopsis

The Shanghai Cooperation Organisation moved into its second decade with an ambitious agenda. Revamping its institutional framework and external relations will strengthen its position beyond Central Asia.

Commentary

IS THE Shanghai Cooperation Organisation (SCO) a vehicle of opposition to American hegemony? When assessing the future of the SCO and who is in the driver's seat, observers often infer that it is an anti-US and anti-NATO organisation. Such conclusions, however, disregard the fact that both the United Nations and the United States recognise the SCO's role in assisting with a spectrum of security issues in Eurasia – the greater Black Sea region and Central Asia.

Initially sceptical, the US Bureau of South and Central Asia noted the potential for enhanced cooperation in countering terrorism in Eurasia during a Beijing Media Roundtable in March 2011. Moreover, the latest report Central Asia and the Transition in Afghanistan, released by Senate Committee on Foreign Relations on 19 December 2011, acknowledges the SCO's role in counter-narcotics efforts. While the SCO has demonstrated its contribution towards regional security, external parties are still puzzled as to who is in charge, and how efficient will be the implementation of the organisation's ambitious goals.

Division of labour

Traditional divisions of labour within the SCO, established by China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan and Uzbekistan in 2001, are arguably reflected in Russia's security agenda, and in China's economic sphere. This view might not hold much longer considering that Beijing, presiding over the SCO in 2011-2012, has shown increased interest in security issues and called for more rapid responses towards security threats.

China's strategic reemergence expands its operational frontier throughout Central-Eastern Asia, through a network of pipelines which guarantee long-term energy supply as long as the transportation of the gas and oil is protected from destabilising forces. This development challenges Russia and the US' long-term strategic interests.

Russia, having lost its strategic advantage over energy transportation in 2010, wants to avoid being pulled southwards, where the US "New Silk Road" strategy lies, and supports the expansion of the SCO's operability

beyond Eurasia towards the Pacific. The division of labour between Russia and China is undergoing a readjustment, where the two larger member states generate initiatives in economic and security areas. The SCO's mechanisms provide a flexible framework for their evolving Central Asian policies, minimising the necessity to compete in these spheres, especially since China has become Russia's primary trading partner. An increase in bilateral trade from $80 billion to $200 billion by 2020 is possible.

Furthermore, after the successful SCO-sponsored conference on Afghanistan attended by the US, EU, the Organisation for Security and Cooperation in Europe (OSCE), G8 and NATO in Moscow in March 2009, the member states showed confidence over the organisation's ability to become a significant discussion platform for not only region-related matters, but also global policy issues, such as "international information security".

Challenges in Cyberspace

In 2008, the SCO Agreement in the field of International Information Security underlined the 'digital gap' between states: the more developed parties 'monopolise' the production of software/hardware, creating dependence on these products from the less developed states whose chances of participating in international information technology collaborations dwindle. Member states believe that the current conventions lack adequate codes of conduct in communications between different countries, omitting a broad spectrum of cyber-security abuses, which could escalate into cyber-conflict. Russia's SCO National Coordinator, Ambassador Barsky described the Council of Europe Convention on Cybercrime (2001), which came to force on 1 July 2004, as less than satisfactory.

Consequently, China, Russia, Tajikistan and Uzbekistan, submitted a draft code of the International Code of Conduct for Information Security before the 66th United Nations General Assembly Meeting on 12 September 2011. This initiative should be viewed in the context of reports singling out Russia and China as among the worst 'culprits' of cyber-attacks; as "aggressive and capable collectors of US economic information and technologies" (Report to Congress on Foreign Economic Collection and Industrial Espionage 2009-2011, Foreign Spies Stealing US Economic Secrets in Cyberspace).

While all parties agree on areas of common concern, such as cyber-crime, they greatly diverge over controlling Internet content. The SCO advocates restraining dissemination of information which provokes the three "evils" (terrorism, extremism, separatism) and preventing other nations from using their core technologies to destabilise economic, social and political stability and security. The external parties, who prefer the use of term "cyber security", rather than "information security", argue that rigid or wrong government regulations can cause more harm to cyberspace security, arguing that private sector engagement is inevitable in the formulation of a constructive international norm.

Beyond Inertia and MoUs

The SCO needs to overcome several obstacles within its evolving institutional framework and in relation to external parties to maintain its momentum in resolving this contested global issue. The organisation should move forward with implementing both the SCO Development Fund, (Russia's proposal), to fund preliminary project studies, and the SCO Bank, (China's suggestion), to fund major projects. The Secretariat, the permanent SCO authority, based in Beijing and relying on employees nominated from the host countries, needs to become the primary recruiter of its staff to preserve continuity within the institutional structure.

Externally, the SCO needs to revamp its PR campaign and educate the professional sphere around the globe regarding its institutional framework and activities. Inter-regional cooperation should move beyond signing Memorandums of Understanding (MoUs) and declaratory statements, to specific projects between regional and international organisations. ASEAN-SCO cooperation is a good case in point.

The two organisations signed the MoU in 2005 at the ASEAN Secretariat in Jakarta, yet as late as December 2011, both Secretariats reported that hardly any exchanges had taken place. An SCO-sponsored Cyberspace Conference could tackle practical issues, such as pledges from governments to curb 'patriotic hackers' and the threats of trans-national cyberspace security violations.

Alica Kizekova is a Teaching Fellow at Bond University in Australia. She was previously a Visiting Associate Fellow at the Centre for Multilateralism Studies, S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University and has also worked as a ministerial adviser in the Slovak government.