Centre for Air Power Studies (CAPS)
Forum for National Security Studies (FNSS)

RUSSIA – CHINA NEXUS IN CYBER SPACE

E. Dilipraj
Associate Fellow, CAPS

On May 08, 2015 Russia and China inked an important agreement in the field of cyber security. This bilateral agreement is the latest entry in the series of agreements which are being signed between Russia and China as a result of their recently established closeness due to common interests and concerns in international politics.

The ongoing turmoil in Ukraine and sanction politics by the West has renewed the hostilities and tensions between Russia and the West. However, to the dismay of the West, Russia has shifted its focus to 'Pivot to Asia', more importantly towards China. It can be stated that common concerns and interests, especially the desire to challenge the pre-eminence of the US has brought both these actors together. Moreover, China's global aspiration on the other hand is not to emerge as a key player in the South Asian Region but at the international affairs level. This contention for global super power status between China and the US has led Beijing to look for powerful allies in international politics and for redefining the strengthening of relations with Russia in a way has reinforced the vigour in the partnership between the two countries. Common national interests and priorities have resulted in a partnership which for the Western allies could be a force to reckon with.

Not confining the rapprochement between Russia and China to just bilateral ties, the partnership has now moved ahead through global participation and engagement. One such initiative undertaken by the two countries recently is on the issue of global cyber security with regard to the global internet governance model. While US and many other western countries, especially the "Five Eyes"[1], propose and push for the multi-stakeholder[2] model of governance for internet, China and Russia together lead another club which proposes for multilateral[3] model of governance. Although it is important and interesting to know the pros and cons of the two proposed models of governance for internet, it however does not come under the purview of this paper. Hence, while excluding the details about the models, it is important to know the reason for the emergence of this debate. In mid-2013, former National Security Agency (NSA) contractor Edward Snowden revealed details of many mass surveillance programmes of the US and other western countries on many sovereign states. This act of breach of sovereignty through the virtual domain has aggravated the debate on internet governance across the globe.

Nevertheless both Russia and China, and also to an extent countries like India, have strongly opposed the business friendly multi-stakeholder model which has resulted in a stalemate for a common consensus to be arrived at the global arena. In the meanwhile, Russia and China, which are well established cyber players of the world, are making their contingency plans and empowering their cyber skills to face more challenges in the vulnerable virtual future. China withdrew from the bilateral cyber working group with the US after the latter accused five Chinese personnel of conducting cyber espionage on the US and demanded extradition to the US for undergoing trials.[4] Similarly, the Russia-US cyber working group is also in a frozen state due to the Ukraine crisis. In September 2014, the Russian President Vladimir Putin was making rigorous plans to move key Russian online infrastructures into its own territories from overseas. Moscow is also preparing plans to keep the Russian part of internet alive even if it is severed externally by its foes in case of emergency war situations in the future. Though the IT specialists of the country are aware of the difficulty involved in it, they are positive about keeping the internet alive if they could get free connection from any of its neighbouring countries.[5] [It is important to note that China and Russia are neighbouring states to each other].

It is at this critical juncture, the bilateral "Agreement on Cooperation in the field of International Information Security" has been signed by both Russia and China on May 08, 2015 in Kremlin, Moscow. The highlights of the key areas of cooperation as identified by the agreement are as follows:

- The establishment of communication channels and contacts for sharing joint response to threats in the sphere of international information security
- Exchange of information and cooperation in law enforcement areas in order to investigate cases involving the use of information and communication technologies for terrorists and criminal purposes
- Cooperation between the competent authorities in the field of critical information infrastructure safety, the exchange of technology and cooperation between the competent authorities of these two states to respond to computer related incidents
- To contribute in improving the international legal framework, and practical mechanisms to ensure cooperation between Russia and China in international information security
- To enhance cooperation and coordination between Russia and China on issues of international information security within the framework of international organizations and forums (including the United Nations, the International Telecommunication Union, the International Organization for Standardization, Shanghai Cooperation Organization, the BRICS countries, Regional Forum of the Association of Southeast Asian security etc.)
- Joint training of specialists, exchange of students from higher educational institutions.[6]

This agreement between Russia and China can be seen as an act of confidence building measure to strengthen their stand in the global cyber politics. Unlike the western media reports which stated that both Russia and China have pledged not to hack each other's networks, the agreement has not mentioned anything related to it. In fact, the document only talks about closer and deeper collaboration and joint response between Russia and China on issues related to cyber security. Although, the document which is available in the open domain mentions that this agreement is not directed against any third country, the global situation and the time in which this agreement has been signed by both the countries give out a different signal. It can be interpreted as an act of covert challenge from Russia and China towards the hegemony of the US and the west on global information security.

While these two world powers have clearly expressed their stand in the global cyber politics, India's stand continues to be ambiguous. India, which is also an important cyber player owing to the sheer size of cyber resource usage in its territory, has not been explicit in terms of its strategy for the future. However, India has not endorsed the US proposed multi-stakeholder model of internet governance, neither has it openly supported the multilateral model that is being backed by Russia and China. Nonetheless, keeping aside the governance debate, it is important to analyse the prospects of having a cyber security arrangement with Russia and China either bilaterally or join the existing agreement with the two countries which otherwise means a trilateral agreement. Such an arrangement between these three countries will not only become an act of confidence building measure between the three entities, but it will also definitely create a strong psychological impact on the West and a possibility of rebalancing the debate on global cyber governance.

(Disclaimer: The views and opinions expressed in this article are those of the author and do not necessarily reflect the position of the Centre for Air Power Studies [CAPS])

End Notes

[1] Five Eyes (FVEY), refers to an intelligence alliance comprising Australia, Canada, New Zealand, the United Kingdom, and the United States. These countries are bound by the multilateral UKUSA Agreement, a treaty for joint cooperation in signals intelligence.

[2] Multi-stakeholder model of internet governance is a proposed model where all the stakeholders from government, businesses, civil society, research institutions and non-government organizations will participate in the dialogue, decision making and implementation of policies.

[3] Multilateral model of internet governance is a proposed model where the governance and decision making related to any issues in cyberspace is left only with the government of the country. This model claims that the influence of private players and civil society can be avoided in the decision making process which otherwise would lead to monopolizing the cyberspace by the civil society.

[4] "China Reacts Strongly to US Announcement of Indictment Against Chinese Personnel, *Spokeperson's Remarks of the Ministry of foreign Affairs of the People's Republic of China*, May 20, 2014, http://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/t1157520.shtml, accessed June 10, 2015.

[5] "Russia to be disconnected from the Internet?", Pravda.ru, September 19, 2014, http://english.pravda.ru/society/stories/19-09-2014/128572-russia_internet-0/#, accessed June 10, 2015.

[6] "Agreement between the Government of the Russian Federation and the Government of the People's Republic of Cooperation in the field of international Information Security", Government of Russian Federation, April 30, 2015.
