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

US – CHINA CYBER CAMARADERIE: A STEP TOWARDS ARMS CONTROL OR CONFIDENCE BUILDING IN CYBER DOMAIN?

Mr E.Dilipraj
Associate Fellow, CAPS

On December 01, 2015, the United States (US) and China held their 'First Cyber Security Ministerial Dialogue' in Washington which is being dubbed as the 'first cyber arms control negotiations' of the world by few reports and analysts. The western reports and analysis which came prior to the meeting compared the cyber dialogue between China and the US with the Cold War era nuclear negotiations between the USSR and the US. Although such comparisons are bound to happen due to the commonalities in their technological capability, the differences however between them, when realised would eventually dilute such comparisons. Moreover, it is too early for any country to go for an arms control negotiations in the cyber realm as the technology is still under development. Therefore, this paper aims to analyse and answer the following questions:

- Was the meeting really a cyber arms control dialogue?
- What led these two countries to hold such a high level meeting?
- Is cyber arms control feasible in these early years of development?

To begin with, the December 01, 2015 meeting was a reflection of the commitment made by the Presidents of both China and the US during President Xi Jinping's state visit to Washington in September 2015. It was during this visit, the leaders of both the countries agreed 'to establish a high-level joint dialogue mechanism on fighting cybercrime and related issues'. [1] The leaders also agreed that this dialogue mechanism would help review the timeliness and quality of responses to requests for information and assistance with regard to malicious cyber activity of concern identified by either side. For the success of this mechanism, the leaders also agreed for the establishment of a hotline to deal with the escalations of issues that may arise in the course of response to requests

from either sides related to cyber issues. Ultimately, both the entities agreed to hold the meetings for this dialogue twice a year starting from December 2015.[2]

Hence, it is clear that the meeting was first step in the series of dialogue to sort out the issues related to cybercrime between the two countries. However, it is important to examine the events that led to the establishment of such a mechanism between the two countries. To start with, both the US and China have for until recently have been blaming each other for various cyber attacks on their respective infrastructures that includes both critical and non-critical. In fact, the frequency of such blame game was higher from the US side against China on many occasions and China has always responded to such blames by portraying itself as a victim of cyber attacks from the US. Few recent incidents worth mentioning are:

In May 2014, the Federal Bureau of Investigation of the US indicted five Chinese military hackers, allegedly members of the secret cyber unit— Unit 61398, with charges of cyber espionage against the US for the period 2006-2014 and instructed the Chinese government to extradite the 'culprits' to stand trial.[3] Claiming these allegations as baseless, the Chinese government used this opportunity and went to the extent of suspending the US-China cyber working group and terminated the process of information sharing with the US on issues related to cyber security.

In June 2015, the US Office of Personnel Management (OPM) announced that there was a serious data breach in its networks and records of millions of personnel information was stolen through cyber means. With initial claims of stolen records starting at around 4 million personnel's, the count eventually increased in the following months to 22.1 million personnel's.[4] The OPM data breach is considered in the US as the worst data breach ever in its history, due to the fact that sensitive data like fingerprints and background information of their personnel had been stolen. Although no official statement or accusation was made on any person, group or state regarding the breach, the prying eyes of the US law enforcement agencies were on China and unofficial statements against China also surfaced on regular intervals. As expected, China denied all allegations against it and portrayed itself as a victim of many such high profile cyber attacks and espionage from the US. In fact, the OPM data breach case was one of the many cases discussed during the first cyber security ministerial dialogue. According to a report by Xinhua News Agency, the official news agency of the Chinese Government, after much deliberation, the US agreed to consider the case as a criminal case rather than a state-sponsored cyber attack.[5]

Based on the above mentioned events, the magnitude of cyber issues persisting between the US and China is evident more in the case of the US as it is battling to address these issues due to lack of a proper channel between the two

countries. It is for this very reason; the current mechanism was proposed and agreed by both the countries. In fact, the background work for establishing such an initiative had started even before Xi's visit when Meng Jianzhu, secretary of the Committee of Political and Legal Affairs (CPLA), CPC Central Committee visited the US in early September 2015. It is claimed by the Chinese source that a five-point consensus was reached during Meng's visit and the ongoing dialogue is aimed in implementing this consensus.[6] Although the actual text of this five-point consensus is not available in the public domain, it can be speculated with certain confidence due to the existence of unsolved complexity and mistrust in the bilateral cyber issues between the US and China that the ongoing dialogue is not in any way related to cyber arms control rather it is an effort mainly from the US in order to constantly engage with China on close quarters as well as to build confidence between the two countries on issues related to cyber.

Finally, while talking about cyber arms control, as mentioned earlier the technology is still under development and it would be detrimental for the growth of technology if any restrictions are to be implemented at this stage. Moreover, it would even be technologically not viable at this juncture to implement such control regimes due to lack of sophisticated cyber forensic mechanisms. Ability to attribute with enough evidences is the aspect that would sustain any allegation of an attack against the perpetrator. In case of a cyber attack using a cyber weapon, with the available forensic technology, it is very difficult to attribute an attack to someone and even if this is achieved, it is more difficult to prove the allegation legally with enough technical evidences. Moreover, no country would want their cyber arsenal to be restricted at this early stage without being tested on ground as it gives them a unique superiority over the rest. Additionally, verification and monitoring mechanisms would also become very complex with the available technology in case of a control regime. Therefore, it can be said that cyber arms control is not a pragmatic approach for securing cyber space at least for a decade rather the countries have to follow certain code of conduct and should enhance confidence building measures for operations, cooperation and co-existence in the cyber world.

(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])

Notes

[1] "FACT SHEET: President Xi Jinping's tate Visit to the United States", Office of the Press Secretary, The White House, Spetember 25, 2015, https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states, accessed on December 19, 2015.

[2] Ibid.

[3] "Five Chinese Military Hackers Charged with Cyber Espionage Against U.S.", *The FBI News Blog*, May 19, 2014, https://www.fbi.gov/news/news_blog/five-chinese-military-hackers-charged-with-cyber-espionage-against-u.s,accessed on December 20, 2015.

[4] "Hacks of OPM databases compromised 22.1 million people, federal authorities say", *The Washington Post*, July 09, 2015, https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/, accessed on December 20, 2015.

[5] "First China-U.S. cyber security ministerial dialogue yields positive outcomes", Xinhuanet, December 02, 2015, http://news.xinhuanet.com/english/2015-12/02/c_134874733.htm, accessed on December 21, 2015.

[6] Ibid.