A VIEW FROM THE "GREAT FIREWALL OF CHINA"

Rapporteur Report for CAPS Fellows' Seminar

By: Uday Deshwal (Research Associate, CAPS)

Chair: Wg Cdr MK Sharma, Research Fellow, CAPS

Speaker: Mr. E Dilipraj, Research Associate, CAPS

Date: 31st October, 2014

Venue: Conference Room, Centre for Air Power Studies, New Delhi.

The seminar saw Mr. E Dilipraj presenting a paper titled, ***'Dragon's Fire in the Virtual World',*** as part of the weekly CAPS Fellows' Seminar. The seminar was chaired by Wg Cdr MK Sharma, Research Fellow, CAPS.

At a time when the strength and scope of China's burgeoning cyber capabilities are a growing cause for concern for a large number of countries across the globe including India, the speaker's paper, in the words of the Chair, was a "descriptive and brave attempt at exploring the '***Great Firewall of China***'", as it looked to provide a technical and methodological understanding of the general Chinese cyber environment and the covert cyber activities being conducted from Chinese soil under the direct and indirect aegis of the Chinese state machinery.

The presentation was broadly divided into three sections:

I. 'Cyber Environment of China'

II. 'Chinese Cyber Terror'

III. 'Chinese Hackers Groups'.

In the first section on the general cyber environment in China, the speaker talked about the growth of Internet in China to the extent of it steadily seeping into the everyday usage of approximately 50% of the population. Consequently, he proceeded towards discussing the presence of stringent and intrusive efforts towards monitoring and censoring its population's internet usage and activities, making it one of only five nations (other nations include Iran, North Korea, Saudi Arabia and Bahrain) in the world which maintain such a level of surveillance over their own populace. After providing a brief look into the contemporary public cyber environment in China, the speaker gave a detailed outline of the rules and methods guiding the implementation of the tools, code named "Golden Shield" aka "Great Firewall of China", that are used by the government and its related agencies for strictly monitoring and manipulating the internet in China. Aside from the various technical methods described, the presenter noted the concerned authorities' use of employing over two million "Internet Opinion Analysts" who further analyse the public opinions percolating in the virtual world in China.

Moving on, the speaker shifted the focus towards the State and military backed cyber activities of China in the section on 'Chinese Cyber Terror'. He emphasized on the fact as to how China considers its cyber capabilities as a national asset, followed by the key purposes that make these capabilities such an added and vital domain of warfare for China. Successively, attention was drawn to the instances of covert attacks carried out against various nations by China in the cyber world. The speaker went on to share the details and his thoughts on the relevant case studies of Chinese cyber attacks on India and the United States of America. In the case of India, two of the instances shared included: a 2012 incident of data from the computers in the Eastern Naval Command having been collected and reportedly sent to a location in China. The disconcert surrounding such a breach was exacerbated by the fact that the Eastern Naval Command is an important strategic target as the INS Arihant, India's indigenously built nuclear powered submarine, was stationed there; a 2013 incident of computers at DRDO being compromised, with the theft of several important files, including ones on the Cabinet Committee on Security (CCS), traced back to a server in China.

The speaker further divulged the nature of the cyber attacks on the US as being specifically focused towards acquiring information and technology for R&D purposes in the industrial and military domain in both the private and government sectors, so much so that in the past decade or so, "unofficial cyber theft has become one of the R&D methods" that China pursues in its quest to rapidly undergo transformation from a developing power to a developed power. All the instances cited by the speaker provided evidence that ratified the Chinese strategy of using covert cyber activities for R&D purposes. One of the major incidents was a series of covert attacks named 'Titan Rain', which involved the collection of sensitive information including theft of specific files, documents and technology from NASA, US Naval War College, Redstone Arsenal Military Base, World Bank, Lockheed Martin, among others.

The Chinese State's direct involvement in these attacks was a matter of debate until, as the speaker very ably revealed, the tracing back of these activities to a network in a building in Shanghai by the US cyber experts in 2006. The building was revealed to be housing a part of a group of cyber experts belonging to Unit 61398, an official unit under the PLA's Cyber Command and was institutionally under the aegis of the Communist Party of China's Central Military Commission, thus revealing the extent of the sheer amount of resources being directed towards covert and strategic cyber attacks by China with complete state and military backing.

The Chinese State and its cyber army, the speaker pointed out next, was not alone when it came to contrastingly (to the strict censoring that the general public faces) indulging in illicit cyber activities from Chinese soil against foreign targets. Over the recent past, China has seen a meteoric rise in the numbers of the hacking community, who as the speaker subsequently explained have a virtual free hand in conducting acts of cyber terror as long as the intended targets lie outside the periphery of Chinese territory. The extent of their attack methods and likely targets was presented through case studies of three of the most prominent hacker groups from China namely the 'Honker Union', 'NCPH' and 'Hidden Lynx'.

In conclusion, the speaker observed the enormous gap that existed between the set of rigorous monitoring norms in place for the general population in China and its own state and military use of the cyber world for various acts of espionage and data collection along with the lack of almost any form of reprimand for the large hacking community attacking foreign targets. Furthermore, a distinction was made between the nature of targets that are attacked by the Chinese state backed cyber army and those attacked by the hacking community. As a parting thought, the speaker highlighted the fact that the presence of such a large hacking community is bound to be a double-edged sword for China.

The following were a few of the issues raised during the subsequent discussion:

- An important point that was brought to the fore was the citing of recent cases of death penalties being awarded to those found guilty of internally committing cyber crimes against Chinese interests and assets. The point underlined the gravity of the problem of rogue hackers and how China itself was a victim of a growing number of cyber crimes, and at the same time also exposed the binary nature of the cyber environment in China.

- One of the other issues discussed was that of the lack of robust attribution technology, and of a general maturity of the cyber forensic systems.

- On the issue of the integration between cyber and other kinetic forms of warfare, it was observed that with the all-encompassing nature of the cyber world, it would actually be preferable to look into ways of disintegrating the two forms.

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

****

Page designed by: Kriti Singh, AF, CAPS