ORF ISSUE BRIEF

MARCH 2013 ISSUE BRIEF # 52

China and Cyberspace

Rahul Prakash

In the absence of a legal framework, Beijing is in overdrive to build its cyberspace capabilities—with military ramifications—as the world looks askance.

Introduction

Today, nations rely on cyberspace for a multitude of functions, including banking, communication, transportation, and for military purposes. Routine breakdowns have shown the extent of damage that can be incurred when these services fail to function. Vulnerabilities in the information networks that support these functions have been exploited by vested interests/an `enemy' country for economic benefits, disrupting critical services, and gaining access to confidential economic and military data. Although China has so far not been directly implicated for perpetrating attacks on computer networks of other countries, investigations in many cases have invariably found it to be the prime suspect. In the past decade, there have been several cyber attacks on critical information systems of countries, including India, which have been traced to China. While most of these attacks were not aimed at destroying the target country's information systems, they enabled the attacker to extract huge volumes of data—sometimes confidential—that could be useful to an adversary country for military and security policy making. China is using cyberspace for several purposes: to upgrade the People's Liberation Army's (PLA) fighting capabilities; to collect intelligence about military and security related activities of other nations; and for economic gains. This Issue Brief examines why China would seek to develop offensive and defensive capabilities in cyberspace, the evidence which suggests that it is developing these capabilities and, finally, it examines China's existing cyber infrastructure.

The PLA and Cyberspace

The development of offensive and defensive capabilities in cyberspace forms part of China's overall military modernisation strategy which emphasises on fighting localised wars under informationised conditions. The Chinese Defence White Paper of 2010 states:

"To meet the new and changing needs of national security, the PLA tries to accentuate modernization from a higher platform. It strengthens the building of a new type of combat capability to win local wars in conditions of informationisation, strengthens the composite development of mechanization and informationization with the latter as the leading factor, focuses informationisation on raising its [PLA's] fighting capabilities based on information systems, and enhances the capabilities in fire power, mobility, protection, support and informationisation."[1]

China is developing a new-age military which would rely on Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) systems to conduct military operations with speed and efficiency. To achieve this, the PLA over the last decade has been developing information systems and networks that would serve as the backbone of its military operations. China's leaders recognised the importance of developing offensive capabilities in cyberspace when the US used information technology during its military operations in the 1990 Gulf War. In this conflict as well as subsequent military campaigns in Iraq and Afghanistan, the US military demonstrated the importance of information technology in its military operations. No wonder, China seeks to develop offensive capabilities that could destroy or disrupt enemy information systems in a conflict situation.

Cyber warfare forms part of China's strategy of "Assassin's Mace", whereby a stronger enemy can be defeated by using asymmetric capabilities. China's cyberspace capabilities should not be seen in isolation but viewed along with other domains of electronic warfare—especially as the PLA seeks to have information dominance in a conflict situation and damage the adversary's information networks to delay or disrupt military response.[2]

Cyber attacks carry with them the option of denial, as it is difficult to attribute an attack to a particular state or actor. Even if the attacks are traced back to a country, it can conveniently blame non-state actors and escape retaliation, as has been shown in several cases. The lack of an international framework on cyberspace also facilitates cyber attacks. It is generally believed that this lacunae provides China with a greater impulse to develop these capabilities.

Cyber Espionage

Apart from exploring options in cyberspace for military purposes, it is widely believed that China has been collecting intelligence on a large scale by hacking into information systems of other countries.

Many attacks on military and national security related information systems of countries, including the US, Japan and India, have been traced to China.

The "Titan Rain" attacks that originated in China had targeted network systems of the US military, NASA and the World Bank, among others.[3] In another attack in 2008-2009, known as Ghostnet, hackers from China infiltrated the network systems of the Indian security establishment, embassies, the Dalai Lama's office and hundreds of other government offices across the world.[4] Some of the attacks have even targeted unclassified network systems; analysts believe that these operations would allow China to build capabilities and enable it to operate in real-time conflict scenarios.[5]

Economic Advantage

Cyber warfare does not have only military implications. Exploiting a country's cyber limitations can also provide economic advantages. Many incidents have shown that China is using cyberspace to get access to information to boost various sectors of its economy.

In a report to the US Congress on economic and industrial espionage, the Office of the National Counter Intelligence Executive revealed that American computer networks holding technology and trade secrets have been facing an "onslaught" of intrusions originating from China. According to the report, the most vulnerable areas include information and communication technology, information about scarce natural resources, military technology (including aerospace) and civilian technologies in energy and health sector.[6] In most of these areas, China has made rapid progress in the last few years. For instance, witness China's strides in the field of outer space utilisation. In November 2011, it was reported that Chinese hackers had "full access" to computers of NASA that controlled as many as 23 spacecrafts.[7] The above report also revealed Chinese cyber attacks on computer systems of global energy and oil companies, targeting data on competitive proprietary operations and financing.

There is substantial evidence supporting the charge that China is engaged in strengthening its cyber warfare capabilities. A white paper by US-based cyber security firm McAfee unearthed in 2011 what analysts believe to be one of the greatest cyber hacking attempts yet—codenamed Operation Shady Rat. The attack, carried on for over five years in certain cases, had targeted 70 government and private agencies across the globe. Forty-nine of the infiltrated networks were based in the US, while others included government institutions and companies in India, UK, Taiwan and South Korea. The report found it "particularly intriguing" that the International Olympic Committee (IOC) and the Sport's Anti Doping Agency were targeted immediately before and after the 2008 Beijing Olympic Games.[8] Although the report does not accuse China, the interest shown by the attacker to target the US, India, Taiwan, South Korea and the IOC led analysts to suspect a Chinese hand.[9]

Moreover, the McAfee report listed several satellite companies that were under attack for months. Clearly, these incidents show that China has the ability to infiltrate classified information systems and extract information to develop its own capabilities.

A glaring evidence of its 'culpability' was accidentally provided by the Chinese themselves. A video footage called "The Cyber Storm Has Arrived," aired on China's Central Television 7 (CCTV-7), showed hackers using Chinese made software to disable a website of Falun Gong (a spiritual organisation banned by the Chinese Government) through an American university Internet Protocol (IP) address. The video clip, which was ostensibly aired to portray the US as a bully in cyber space and the need for China to beef up its cyber warfare capabilities, revealed that the software used for the attack was developed at the Electrical Engineering University of PLA.[10]

In February 2013, American information security firm Mandiant stated in a report that PLA Unit 61398 was responsible for cyber attacks on more than 140 companies in over 20 industries worldwide since 2006. Allegedly, the unit operates out of a building in Shanghai and employs "hundreds or perhaps thousands of people." Although these allegations have been rejected by the Chinese government, Mandiant believes that the unit is just the tip of the iceberg and cautioned that there could many more such units.

PLA and the Civilian IT Sector in China

The PLA has turned to various resources in the country to augment its cyberspace capabilities. It utilises underground hacker networks for recruitment, legitimate domestic information technology companies to gain access to technology that would not be available to it in the normal course and research and development work by academic institutions.

In the summer of 2005, a report revealed that the PLA conducted a series of hacker competitions at the regional and provincial levels, possibly to screen and hire recruits for Computer Network Operations (CNO). Similarly, job vacancy announcements were made on two of the most prominent Chinese hacking forums in 2007-2008, for the Ministry of Public Security's (MPS) First Research Institute.[11] Chinese embassies, including in the US, have been recruiting Chinese IT graduates from universities, purportedly for public security—but essentially for computer network operations.[12]

Reportedly, many Chinese from the hacking community have set up legitimate information security firms and developed close links with the PRC government. These organisations get the opportunity to develop new software and advance their technology—legitimately—allowing them to openly work with the government. The Chinese government, on its part, invests in these IT organisations hoping to reap benefits at a later stage and also target fresh recruits. Two companies with which Beijing has developed close links are Topsec and Venustech. A US State Department circular of June 2009 stated,

"there is a strong possibility that the PRC is harvesting the talents of its private sector in order to bolster offensive and defensive computer network operations capabilities."[13]

In 2005, Huawei, a major Chinese software and hardware company, had signed a deal with UK telecom company British Telecom (BT). A British intelligence report in 2009 claimed that Huawei had close links with the PLA and had received huge investments from the Chinese government when it was formed. The British intelligence agencies feared that Huawei components used by BT may contain malicious software that could be activated at a later stage.[14] In a more recent incident, Huawei claimed during an international conference in Dubai that it was able to hack into US and international telecommunications networks and intercept data, which it said was "malicious". In a powerpoint presentation, it said that it had capabilities in "in-depth traffic analysis to enhance network control."[15] Not surprisingly, these claims alarmed the delegates. It would not be surprising if these capabilities and technologies are being shared with the PLA.

China's cyber infrastructure

Like in many other aspects of China, information about its cyber infrastructure—particularly that of the PLA—is not easily available. From what is in the public domain, China's cyberspace infrastructure can be divided into two categories—infrastructure with the PLA and infrastructure with civilian and private sector institutions. However, it is true that the latter work closely with the PLA on various issues—from developing technology to contributing manpower.

The Third and Fourth Departments of the PLA General Staff Headquarters are responsible for cyberspace operations. The Third Department, traditionally responsible for signals intelligence gathering, is believed to be entrusted with computer network defence and intelligence gathering. It exploits the loopholes in the information networks of targets. It is supported by an array of technical reconnaissance bureaus and research and development organisations. Today, the Third Department of the PLA has direct authority over more than 12 operational bureaus, eight of them clustered in Beijing. It also has research institutes supporting its development (See Figure 1).[16]

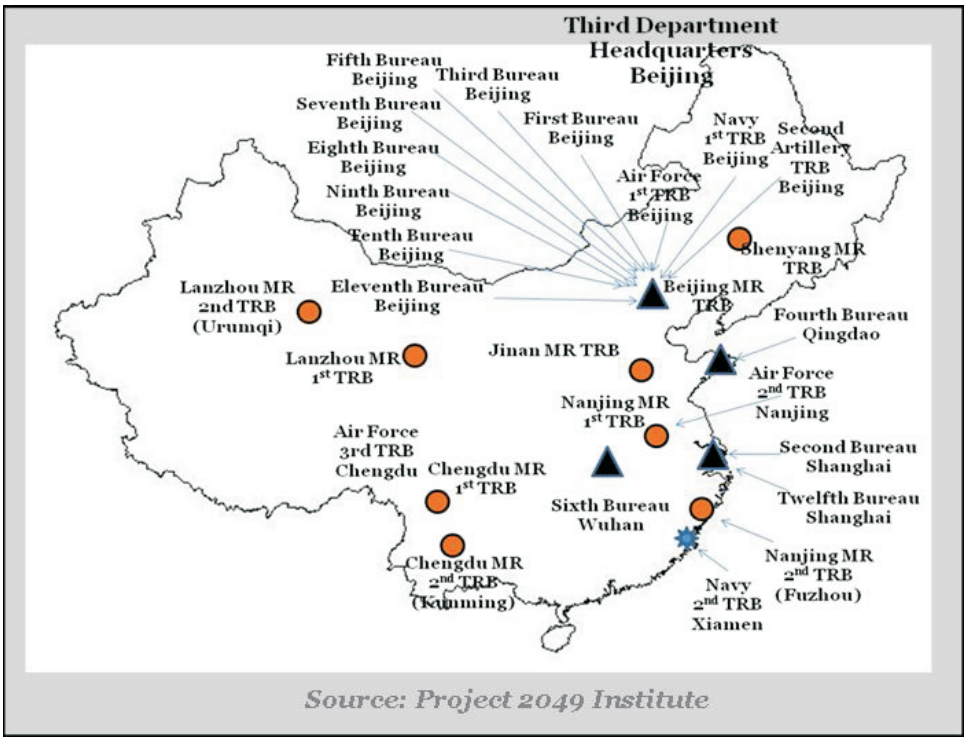
The PLA's Fourth Department is tasked with conducting offensive computer network operations. Presently, there are at least four bureaus, one brigade and two regiments under the Fourth Department.[17] It is affiliated with civilian organisations, including the China Electronic Technology Corporation (CETC) which conducts R&D in electronic and information products.[18] The Fourth Department is also responsible for the PLA Electronic Engineering Academy in Hefei which acts as the PLA's "primary academic training centre for electronic warfare."[19]

The counterparts of the Third and Fourth Departments exist in the PLA's Military Regions (MR), Navy, Air Force and the Second Artillery Force. Each MR reportedly has control of at least one

Technical Reconnaissance Bureau (TRB). The TRBs under the PLA Air Force conduct airborne reconnaissance and monitor air activity and communications of neighbouring air forces. The PLA Navy's TRBs are located in Beijing and Xiamen and control other subordinate offices located nearby. The Second Artillery's TRB is also reported to be based in Beijing.[20]

Information security organisations, sometimes branched from civilian institutions in China, are also affiliated with the PLA. The China North Computation Centre, National Research Centre for Information Security Technology, Information Security Research Institute and the National Information Security Engineering Technology Centre are among these organisations.[21]

Figure 1



Source: Mark A. Stokes, Jenny Lin and L.C. Russell Hsiao, The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure, Project 2049 Institute.

Conclusion

There is enough evidence to suggest that China is aggressively augmenting its offensive capabilities in cyberspace. At the same time, with the PLA modernising to fight wars under "informationised" conditions, it will, like other militaries, become dependent on cyberspace for its military operations. It will also focus on advancing its defensive capabilities to thwart attacks on its own systems during a conflict and in peacetime. China, which has the highest number of internet users, is also facing challenges from domestic hackers. Whatever technology China develops to protect its domestic assets, will definitely play a crucial role in augmenting the PLA's cyber warfare capabilities. The Chinese private sector will continue to play a crucial role in securing cyberspace.

The PLA is reportedly creating a more centralised command structure for information warfare. Cyber warfare will be integrated with other modes of electronic warfare which will form a part of PLA's plans to prepare for conflicts under "informationised" conditions. According to a report submitted to the US Congress, "Earlier in the past decade, the PLA adopted a multi-layered approach to offensive information warfare that it calls Integrated Network Electronic Warfare or INEW strategy. Now, the PLA is moving toward information confrontation as a broader conceptualization that seeks to unite the various components of IW under a single warfare commander. The need to coordinate offensive and defensive missions more closely and ensure these missions are mutually supporting is driven by the recognition that IW must be closely integrated with PLA campaign objectives." [22]

Till legally binding international norms regarding conduct in cyberspace—covering all aspects including cybercrime, cyber espionage and cyber warfare—are put in place, China in all likelihood will continue to build on its capabilities and exploit the loopholes in the military and economic information infrastructure of other countries.

ABOUT THE AUTHOR

Rahul Prakash is a Junior Fellow at Observer Research Foundation. His research interests include technology and security, Chemical, Biological, Radiological and Nuclear (CBRN) issues and security developments in Asia. He has co-authored a report on *Chemical, Biological and Radiological Materials: An Analysis of Security Risks and Terrorist Threats in India*, an outcome of a joint study conducted by ORF and the London-based Royal United Services Institute. He has also published Issue Briefs on China's progress in Space and rise of microblogs in China. He has done BA (Hons.) Political Science from Delhi College of Arts and Commerce, Delhi University and holds a Post Graduate degree in International Relations. He has been working with ORF since December 2010. He can be reached at rahulprakash@orfonline.org

Endnotes:

1. Information Office of the State Council, People's Republic of China, *China's National Defense in 2010*, March 2011, Beijing, available at http://english.gov.cn/official/2011-03/31/content_1835499.htm (accessed on June 20, 2012).
2. Northrop Grumman, Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation, Report Prepared for the US-China Economic and Security Review Commission, 2009, available at http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf (accessed on February 28, 2012).
3. Nathan Thornburgh, "The Invasion of Chinese Cyberspies," The Time, August 26, 2005, available at http://www.guardian.co.uk/technology/2010/sep/24/stuxnet-worm-national-agency (accessed on April 05, 2012).
4. Mike Harvey, "Chinese hackers using ghost network to control embassy computers," The Sunday Times, March 30, 2009, available at http://www.timesonline.co.uk/tol/news/uk/crime/article5996253.ece (accessed on April 07, 2011).
5. Robert Marquand and Ben Arnoldy, "China Emerges as Leader in Cyberwarfare," *Christian Science Monitor*, September 14, 2007, available at http://web.mit.edu/gssd/cyberspace/Weekly%20Article/China%20emerges%20as%20leader%20in%20cyberwarfare.pdf (accessed on June 12, 2012).
6. Office of the National Counter National Intelligence Executive, *Foreign Spies Stealing US Economic Secrets in Cyberspace*, October 2011, available at http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf (accessed May 13, 2012).
7. "Chinese Hackers had Full Access to NASA Lab that Commands 23 Spacecraft," *Daily Mail*, March 07, 2012, available at http://www.dailymail.co.uk/sciencetech/article-2110506/Chinese-hackers-control-Nasa-lab-commands-23-spacecraft.html (accessed on May 15, 2012).
8. McAfee, *Revealed: Shady Rat*, 2011, available at http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf (accessed on May 21, 2012).

9. Michael Joseph Gross, "Operation Shady rat—Unprecedented Cyber-espionage Campaign and Intellectual-Property Bonanza," *Vanity Fair*, August 02, 2011, available at http://www.vanityfair.com/culture/features/ 2011/09/operation-shady-rat-201109 (accessed on May 22, 2012).

10. Matthew Robertson and Helena Zhu, "Slip-Up in Chinese Military TV Show Reveals More Than Intended," The Epoch Times, August 28, 2011, available at http://www.theepochtimes.com/n2/index2.php?option=com_content&task=view&id=60619&pop=1&page=0&Itemid=1 (accessed on April 02, 2012).

11. Northrop Grumman Corporation, Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation, Report submitted to the U.S.-China Economic and Security Review Commission, 2009.

12. Willy Lam, "Beijing Beefs Up Cyber-warfare Capacity," *Asia Times*, February 09, 2010, available at http://www.atimes.com/atimes/China/LB09Ad01.html (accessed on June 14, 2012).

13. "Chinese firm hired Blaster hacking group, says U.S. cable," China Defense Mashup, December 07, 2010, available at http://www.china-defense-mashup.com/chinese-firm-hired-blaster-hacking-group-says-us-cable.html (accessed on Feb 25, 2011).

14. Michael Smith, "Spy Chiefs Fear Chinese Cyber Attack," The Sunday Times, March 29, 2009, available at http://www.timesonline.co.uk/tol/news/uk/article5993156.ece (accessed on March 07, 2011).

15. F. Michael Maloof, "China Tech Company Brags: We Hacked U.S. Telecoms," *WND.Com*, June 14, 2012, available at http://www.wnd.com/2012/06/china-tech-company-admits-hacking-u-s-telecoms/ (accessed on June 25, 2012).

16. Mark A. Stokes, Jenny Lin and L.C. Russell Hsiao, *The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure*, Project 2049 Institute. November 11, 2011.

17. Ibid

18. Northrop Grumman Corp, *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage*, Report prepared for the US-China Economic and Security Review Commission, March 7, 2012, available at http://www.uscc.gov/RFP/2012/USCC%20Report_Chinese_CapabilitiesforComputer_NetworkOperationsandCyberEspionage.pdf (accessed on June 02, 2012) and "Company Overview of China Electronics Technology Group Corporation," *Bloomberg Businessweek*, July 05, 2012, available at http://investing.businessweek.com/research/stocks/private/snapshot.asp?privcapId=25107944

19. Northrop Grumman Corp, *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage*, Report prepared for the US-China Economic and Security Review Commission, March 7, 2012, available at http://www.uscc.gov/RFP/2012/USCC%20Report_Chinese_CapabilitiesforComputer_NetworkOperationsandCyberEspionage.pdf (accessed on June 02, 2012).

20. Mark A. Stokes, Jenny Lin and L.C. Russell Hsiao, *The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure*, Project 2049 Institute, November 11, 2011.

21. Ibid.

22. Northrop Grumman Corp, *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage*, Report prepared for the US-China Economic and Security Review Commission, March 7, 2012, available at http://www.uscc.gov/RFP/2012/USCC%20Report_Chinese_CapabilitiesforComputer_NetworkOperationsandCyberEspionage.pdf (accessed on June 02, 2012).

Observer Research Foundation,
20, Rouse Avenue, New Delhi-110 002
Phone: +91-11-43520020 Fax: +91-11-43520003
www.orfonline.org email: orf@orfonline.org