CHINA'S MILITARY AND SATELLITE INTELLIGENCE PROGRAMME

DHRUBAJYOTI BHATTACHARJEE

INTRODUCTION

The idea of Chinese intelligence takes birth from the historic writings of Sun Tzu (*Art of War*) which bears a remarkable similarity to US definitions of intelligence functions and goals. Sun Tzu taught that "fore-knowledge" (*xianzhi*) allowed commanders to outmanoeuvre opponents. Mentioned as the eyes and ears of the dragon, Chinese intelligence gathering depends on technology, manpower, as well as developing and nurturing foreign assets. More modern definitions range from "activating [catalytic] knowledge" (*jihuo zhishi*) to information to protect national security, domestic stability, or corporate interests in a competitive environment.[1] For the Chinese, intelligence is transmittable (*chuandi xing*) and comprises knowledge that satisfactorily (*manzu xing*) resolves a specific decision-making problem.[2]

Dr **Dhrubajyoti Bhattacharjee** is a Research Fellow at the Indian Council of World Affairs (ICWA), New Delhi. Prior to joining ICWA, Dr Bhattacharjee was an Assistant Professor at the Department of Political Science, Siliguri College, University of North Bengal for ten years (2005-15).

1. Chen Jiugeng, "*Guanyu qingbao he xinxi* [Regarding Intelligence and Information]," *Qingbao Zazhi (Journal of Information),* vol.19, no. 1, January 2000, pp. 4–6 as cited in Peter Mattis, "The Analytic Challenge of Understanding Chinese Intelligence Services", *Studies in Intelligence,* vol. 56, no. 3, September 2012, p. 49.
2. Yan Jinzhong, "*Junshi qingbao xue*" [The Study of Military Intelligence] (Beijing: Shishi chubanshe, 2003), p. 12; Cheng Lei, "*Qingbao yuan yu qingbao genyuan* [Intelligence Sources and Intelligence's Roots]," *Tushuguan zazhi [Library Journal]*, No. 3 1994, 16–18, as cited in Mattis, Ibid., p. 49

The manner in which Chinese espionage has developed reflects the traditional Chinese hallmarks of patience and persistence as well as the centuries old Chinese custom of "*guanxi*," the cultivation and use of personal networks to influence events and engage in various ventures.

The three main Chinese intelligence gathering methods often overlap. One is the "human wave" or "mosaic" collection, which involves assigning or dispatching thousands of assets to gather a massive amount of available information. Another is recruiting and periodically debriefing Chinese-born residents of other countries in order to gather a deeper level of intelligence on more specific subjects. The third method is patiently cultivating foreign assets of influence for long-term leverage, insight and espionage.[3] The manner in which Chinese espionage has developed reflects the traditional Chinese hallmarks of patience and persistence as well as the centuries old Chinese custom of "*guanxi*," the cultivation and use of personal networks to influence events and engage in various ventures.[4]

CHINESE INTELLIGENCE STRUCTURE FOR EXTERNAL SURVEILLANCE

The role and fast spreading network of intelligence agencies and designated and dedicated divisions of the People's Liberation Army (PLA), procuring and developing precision-guided equipment, has created a new need for assessing the structure and functioning of these agencies.[5] While these

3. "Espionage with Chinese Characteristics", Intelligence Services Part I, *Stratfor Global Intelligence*, March 2010, p. 2, https://wikileaks.org/gifiles/attach/133/133464_INTEL_SERVICES_CHINA.pdf. Accessed on May 2, 2018.
4. Fred Burton and Scott Stewart, "China: Guanxi and Corporate Security", *Security Weekly*, January 16, 2008, https://worldview.stratfor.com/article/china-guanxi-and-corporate-security. Accessed on May 2, 2018.
5. Luo Tianwen, Liu Ying, Liu Shoushuo, Tan Haifeng, and Wu Di, "Junshi qingbao gongzuozhong mubiao yaohai panding yanjiu," *Qingbao Zazhi (Journal of Information)* vol.29, no. 6, June 2010, pp.107-109.

divisions have been known as "China's CIA,"[6] the Party's need for more intelligence support would have created pressure for such organs to focus more on intelligence requirements rather than the national policy-makers.[7]

China's intelligence services may not be as famous as the Central Intelligence Agency (CIA) or the Russia Intelligence Agency (KGB), but their operations are widespread and well known to counter-intelligence agencies throughout the world.

China's intelligence services may not be as famous as the Central Intelligence Agency (CIA) or the Russia Intelligence Agency (KGB), but their operations are widespread and well known to counter-intelligence agencies throughout the world. The operations of intelligence gathering and their processing being divided within various groups, the Chinese intelligence mechanism has turned into a major force to reckon with. Initially, the Social Affairs Department (SAD), under the Communist Party, was the principal intelligence and counter-intelligence organ. With the creation of the People's Republic, the SAD got absorbed in the Ministry of Public Security (MPS), while the PLA had its own Military Intelligence Department (MID). During the mid-1950s, the Central Investigation Department (CID) was deputed the foreign responsibilities of SAD. Though it got disbanded after the Cultural Revolution, it became functional again during the governance of Deng Xiaoping. The Ministry of State Security (MSS) was created in 1983 by Deng in a merger of the CID and the counter-intelligence elements of the MPS.[8]

Being governed strictly under a single party dictatorship, in China the responsibility of gathering, assessing, as well as taking actions on domestic intelligence is done through its Communist Party Central Committee, the Ministry of State Security (MSS) or *Guojia Anquan Bu (Guoanbu)*, the Ministry of Public Security (MPS) or *Gong An Bu* (which mostly caters to domestic

6. Kan Zhongguo, "Intelligence Agencies Exist in Great Numbers, Spies Are Present Everywhere; China's Major Intelligence Departments Fully Exposed," *Chien Shao (Hong Kong)*, January 1, 2006.
7. Ian Easton and Mark Stokes, "China's Electronic Intelligence (ELINT) Satellite Developments: Implications for U.S. Air and Naval Operations," Project 2049 Institute, *Occasional Paper*, February 23, 2011.
8. Tainwen, et.al., n.5, p. 3.

intelligence) and the People's Armed Police (PAP). However, due to the opaque nature of China's executive leadership, it is difficult to determine exactly where, or with whom, the intelligence authority really lies. *Guoanbu*, with the cooperation of MPS, handles counter-intelligence, the former being the primary intelligence organisation. Bugging embassies and surveillance of embassy employees or those travelling on diplomatic passports is a common practice for the MSS.[9]

The MSS is also deputed the responsibility of recruiting intelligence officials, especially students from the Beijing University of International Relations. It also runs an internal security department known as the Ninth Bureau for Anti-Defection and Counter-Surveillance to check for moles from within the system. These intelligence officials are deputed to handle a legion of agents (usually known as assets or operatives), comprising Chinese nationals travelling abroad, or residing abroad, or born outside China or even foreign nationals. They are employed on short-term or long-term basis. In the new millennium, it has started employing non-Chinese government officials of other nations. It has also made massive acquisitions of technology for surveillance and information gathering. This is done either by acqusition of targeted technologies by personnel travelling abroad, or by purchasing the foreign firms producing the required technology or using front companies, especially located in Hong Kong, for procuring the desired technologies.[10]

The Military Intelligence Department (MID), also known as the Second Department or *Er Bu* of the People's Liberation Army, primarily focusses on tactical military intelligence. It has the responsibility of acquiring foreign technology to strengthen China's military capabilities. The First Bureau of the MID is responsible for gathering Human Intelligence (HUMINT) overseas and focusses, like the MSS Third Bureau, mainly on Taiwan, Hong Kong and Macao. It is responsible for obtaining much of the technological intelligence used to improve China's military capabilities and for finding customers for Chinese arms exports. The MID's Third Bureau is made up of military

9. Ibid., p.4.
10. Ibid., p.6.

attaches serving in overseas embassies. The Fourth, Fifth and Sixth Bureaus all handle the analysis of different world regions. Another unnumbered MID bureau disseminates intelligence to military officers and China's Central Military Commission (CMC).

The MID's "Seventh Bureau" is the Bureau of Science and Technology. This is where China's vaunted "cyber-intelligence" operations are designed and managed with the help of six government-linked research institutes, computer centres and legions of personal hackers. While not part of the MID, the Third Department of the PLA is another intelligence organisation that handles Signals Intelligence (SIGINT).

The MID's "Seventh Bureau" is the Bureau of Science and Technology. This is where China's vaunted "cyber-intelligence" operations are designed and managed with the help of six government-linked research institutes, computer centres and legions of personal hackers.

On the international and regional platforms, the following divisions play their specific roles as enumerated below.

- **8341 Unit – Central Security Regiment:** This provided security to Mao Zedong and the top political functionaries. It was responsible for the arrest of the Gang of Four in 1976, and was later disbanded after Mao's death.
- **First (Intelligence) Department – [1PLA] – General Staff Department (GSD) First Department:** Being one of the first divisions of operation, this division is delegated to collect information on the Beijing area, Guangzhou region, Nanjing area, Shenyang and Shanghai regions. It also has the responsibility of collecting information from Taiwan, Macao and Hong Kong, and was well known as the "Autumn Orchid" during the 1980s.[11]
- **Second (Intelligence) Department – [2PLA] – GSD Second Department:** This division assimilates military Human Intelligence (HUMINT), Signals Intelligence (SIGINT) and Imagery Intelligence (IMINT) data,

11. William Hagestad II, *21st Century Chinese Cyberwarfare* (IT Governance Publishing, 2012), pp. 164-165.

and disseminates finished intelligence products to the Central Military Commission (CMC) and other consumers; it focusses on scientific and technological intelligence in the military field; and training intelligence personnel.[12]

- **Third Department – (3PLA) – GSD Third Department:** This controls SIGINT; monitors telecommunications of foreign armies; functions through communications stations placed within mainland China as well as in Chinese operations abroad; is responsible for cyber attacks and jamming; monitors the Political, and Logistics Departments, Science and Technology (S&T) and intelligence; oversees the 56th, 57th and 58th Research Institutes; manages or is affiliated with, the PLA Communications Security Bureau, China North Computation Centre, Third Department Computing Centre, National Research Centre for Information Security Technology, PLA Information Security Evaluation and Certification Centre, Information Security Research Institute, National Information Centre and National Information Security Engineering Technology Centre; it also assists in operating the Military Branch Technical Reconnaissance Bureau (MB TRB) of the PLA Air Force (PLAAF) and PLA Navy (PLAN), their headquarters, located in Changping district and Beijing's Haidian district.[13]
- **Fourth Department-(4PLA)-GSD Fourth Department:** This controls the Electronic Counter-Measure (ECM), Electronic Warfare (EW) and the radar of the General Staff Headquarters Department (GSHD); is involved in Research and Development (R&D); the Electronic Intelligence (ELINT) apparatus within SIGINT; cyber warfare, computer network attack and jamming; satellite jamming regiments; space-based reconnaissance and collection of imagery; four bureaus, one brigade and two regiments; manages or is affiliated with China Electronic Technology 18 Corporation (CETC), 29th Research Institute (Chengdu, Sichaun province), 36th

12. Second [Intelligence] Department, Federation of American Scientists, April 15, 2000. http://fas.org/irp/world/china/pla/dept_2.htm; Hagestad. Ibid., pp.163-164.
13. 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, http://project2049.net/documents/pla_third_department_sigint_cyber_stokes_lin_hsiao.pdf; Third Department, Federation of American Scientists, April 15, 2000, http://fas.org/irp/world/china/pla/dept_3.htm; Hagestad II, n.11, pp.151-154;

Research Institute (Hefei, Anhui province), PLA Electronic Engineering Academy (Hefei, Anhui province); and defends command bunkers in the Xishan Western Hills of Beijing. Its functions are assisted by the Southwest Institute of Electronic Equipment (SWIEE) and the MEI 54th Research Institute with headquarters in Ta Yuan, southeast of the Summer Palace.[14]

Fig. 1: Military Intelligence Department[15]

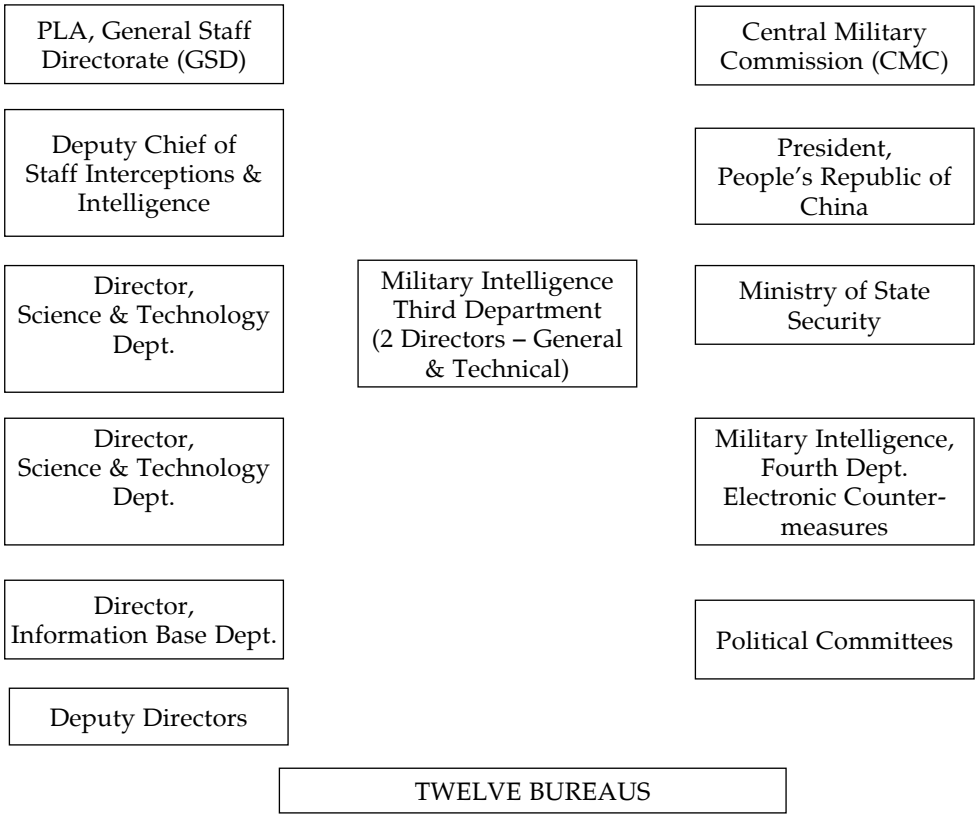

Fig. 1 above depicts the governing or organisation structure of the military intelligence which also oversees the satellite intelligence programme.

14. I. C. Smith and Nigel West, *Historical Dictionary of Chinese Intelligence* (Scarecrow Press, 2012), pp. 96-97; Lowell Dittmer and Maochun Yu, eds., *Routledge Handbook of Chinese Security* (Routledge 2015); Fourth Department, Federation of American Scientists, April 15, 2000, http://fas.org/irp/world/china/pla/dept_4.htm; Hagestad II, Ibid., pp.155-162.
15. Ibid., p. 167.

This chart pre dates the recent military reorganisation but the intelligence organisational structure remains as described.

SPACE-BASED SIGINT AND ELINT

For over 40 years, space-based SIGINT has been a critical component of the global and regional surveillance architecture. Within the broad domain of SIGINT, ELINT has proven to be an effective means of assessing a foreign military's electronic order of battle, including ground-based air defence radars and maritime surveillance systems. Ground and air-based, ELINT assets in space offer a wider field of view and broader geographical coverage.[16]

In a maritime context, notional targets could include radar systems such as the AN/SPS-48, AN/SPS-49, sea-based X-band radar, and AN/SPY-3 emitters. Targeted land-based air surveillance radar systems could include ground-based X-band radar (GBR-X), PATRIOT AN/MPQ-53, AN/TPS-75, and Upgraded Early Warning Radar (UEWR) systems operating in the Ultra High Frequency (UHF) portion of the frequency spectrum.[17]

The Third Department, as the figure above depicts , has been designated to assist, operate as well as coordinate the SIGINT as well as the ELINT operations of China. The twelve bureaus that operate under the PLA are as follows:

- **First Bureau (61786 Unit):** The unit has a more functional than a regional mission. It includes decryption, encryption, and other information security tasks.[18]
- **Second Bureau (61398 Unit):** Probably targets the United States and Canada, gathering political, economic and military-related intelligence. This bureau also supports mobile missions. [19]
- **Third Bureau (61785 Unit):** Has a functional mission which may be collection of line of sight radio communications, including border control

16. Ian Easton and Mark A Stokes, "China's Electronic Intelligence (ELINT) Satellite Developments: Implications for U.S. Air and Naval Operations", *Project 2049 Institute*, Virginia, February 23, 2011, p. 2.
17. Ibid.
18. "Han Yiming", Qinhuangdao Government Website, June 23, 2008, http://121.22.8.170:81/content.jsp?code=188/2008-00006&name=.
19. Stokes, et. al., n.13, p.8.

networks, as well as direction finding, and emission control and security.[20] It is also involved in counter-drug operations. [21]

- **Fourth Bureau (61419 Unit):** Focussed on Japan and Korea.[22]
- **Fifth Bureau (61565 Unit):** Appears to have Russia related missions.[23]
- **Sixth Bureau (61726 Unit):** Seems to have a Taiwan and South Asia mission.[24]
- **Seventh Bureau (61580 Unit):** The mission of the bureau remains unspecific, with possible specialisation in computer network defence and attack.[25] One study of the bureau examined Support Vector Machine (SVM) applications for detecting intrusion patterns.[26] Another studied assessment of the future of the internet and Dense Wavelength Division Multiplexing (DWDM).[27] Another study focussed on the psychological and technical aspects of reading and interpreting a written foreign language,[28] while another dealt with the legal aspects of the global economy.[29]
- **Eighth Bureau (61046 Unit):** It appears to focus on Western and Eastern Europe and perhaps the rest of the world (e.g. Middle East, Africa, and Latin America).[30]
- **Ninth Bureau:** The most opaque body amongst all the bureaus of the department. It is considered to be the primary strategic intelligence

20. Ibid.
21. "Advanced on the National Anti-Drug Effort", *China Network*, June 2, 2007, http://www.china.com.cn/law/zhuanti/yldp/2007-06/02/content_8332019.htm.
22. Stokes, et.al., n.13, p.8.
23. Ibid.
24. Ibid., p.9.
25. "Diverse Language Identification Method", *Journal of Computer Applications*, 2005, 25, http://d.wanfangdata.com.cn/periodical_jsjyy2005z1172.aspx.
26. Li Jian, Jiang Chengshun, and Dong Liying, "Data Type Recognition Based on Selective Integration of SVM", *Computer Engineering*, vol 36, 13, 2010, http://d.wanfangdata.com.cn/Periodical_jsjgc201013064.aspx
27. Wang Qi and Dan Jun, "Network Centric Warfare Development and Technology Strategy", Information Assurance and Communications Security, December 2005, pp. 82-84, http://www.lw23.com/pdf_90d61a36-6c45-48bc-b6c2-4e2ddc8edbb8/lunwen.pdf
28. Zhang Ya'nan and Chen Tao, "Psychological Mechanism of Analyzing Foreign Language Reading", *Sciences and Wealth*, 2011, 3, http://d.wanfangdata.com.cn/periodical_kxycf201103095.aspx
29. Zhang Lidong, "New Developments in Economic Globalization and International Economic Law", *Law and Society*, 2009, 33, http://d.wanfangdata.com.cn/periodical_fzysh200933235.aspx
30. "Recognizing Top Translators for 2009", China Translators Association website, http://www.tac-online.org.cn/ch/tran/2010-12/09/content_3888394.htm

The GSD Third Department oversees a vast bureaucracy responsible for monitoring foreign communications, assuring the security of PLA computer and communications networks, and conducting cyber surveillance on priority targets around the world. If information is power, then the GSD Third Department represents one of the most powerful bureaucracies in China today.

analysis and/or data base management entity and may be involved in audio-visual technology and large scale data base management.[31]

- **Tenth Bureau (61886 Unit):** Also sometimes referred to as the '7911' Unit[32], it appears to have a Central Asia or Russia-related mission, perhaps focussed specifically on telemetry and missile tracking and/or nuclear testing.[33]
- **Eleventh Bureau (61672 Unit):** Also sometimes referred to as the '2020' Unit[34], and having the presence of Russian linguists, this appears to indicate Russia related missions.[35]
- **Twelfth Bureau (61486 Unit):** *This appears to have a functional mission involving satellites, likely inclusive of intercept of satellite communications and possibly space-based SIGINT collection*.[36] It works in collaboration with institutes working on weather satellites, that must have dual use capabilities, bearing SIGINT and ELINT payload.[37]

31. "Gong' An Intelligence Department and GSD Establish an Intelligence Analysis Cooperative Mechanism", Chinese People's Public Security University website, June 28, 2010, http://www.cppsu.edu.cn/cfm_data/shownews_dw.cfm?newsid=1656&fyear=2010; "Public Security Intelligence Section and General Staff Department Establish Seminar Cooperation Mechanism", Public Security Website, June 28, 2010, http://www.cppsu.edu.cn/cfm_data/shownews_dw.cfm?newsid=1656&fyear=2010.
32. Stokes, n.13, p.10.
33. Tao Wenzhao, *History of US-China Relations*, vol. 2, 1972-2000, Chapter 5: Peaceful Development, 1972-2000), (Shanghai: People's Publishing, 2004), http://ias.cass.cn/show/show_project_ls.asp?id=733
34. "Postal Code for 61762 Unit", Postal Code Net.
35. "Deputy Directors of the City People's Congress", December 6, 2005, http://www.jzsrd.gov.cn/news_view.asp?newsid=234.
36. "Human Resources Information", Kunshan Human Resources Market, Official Webiste, http://www.kshr.cn/ksasp/unit/SHOWEMPL.ASP?employee_id=660550.
37. "Meeting on Fengyun-3 Ground Application System Held", *Shinetek*, June 14, 2011, http://www.shinetek.com.cn/Cn/View/Company/NewsDetail.aspx?NewsID=100016.

The GSD Third Department oversees a vast bureaucracy responsible for monitoring foreign communications, assuring the security of PLA computer and communications networks, and conducting cyber surveillance on priority targets around the world. If information is power, then the GSD Third Department represents one of the most powerful bureaucracies in China today. Among its sources of strength is the country's largest pool of well trained linguists specialised in niche areas, such as banking and financial transactions, military activities, energy, and diplomatic exchanges.[38]

Key word and voice recognition technology and large data bases permit greater efficiency in collection, directed against specific targets. Advanced computing facilitates breaking of all but the most sophisticated encryption and passwords. The linkage between computer network operations and the PLA's psychological warfare training units appears reasonable.

The combination of SIGINT and CNE (Computer Network Exploitation), for example, fusing transcripts of phone conversations with intercepted email exchanges, would enable a powerful understanding of the plans, capabilities, and activities of an organisation or individual in near real-time. Key word and voice recognition technology and large data bases permit greater efficiency in collection, directed against specific targets. Advanced computing facilitates breaking of all but the most sophisticated encryption and passwords. The linkage between computer network operations and the PLA's psychological warfare training units appears reasonable. Monitoring of communications, email accounts, websites, and internal networks could support sophisticated perception management operations. [39]

In addition to Third Bureau collection operations, the Third Department's 12th Bureau assets are dedicated toward intercept of foreign satellite communications. In addition to intercepting satellite communications from sites around China's periphery, the 12th Bureau may also operate specialised

38. Stokes, et.al., n.13, p.15.
39. Ibid.

equipment onboard satellites that are capable of intercepting communications around the world from Chinese space-based systems.[40]

While discussing SIGINT capabilities, there is a need to understand the impact of ELINT capabilities as well. Use of the doctrinal concept of integrated network and electronic warfare implies an attempt to link computer network attack and jamming, presumably under the purview of the GSD Fourth Department, which has overall responsibility for EW, including ELINT and tactical Electronic Support Measures (ESM).[41]

An unconfirmed Chinese source indicates that the country's first experimental ELINT satellite—the Shijian-1—was launched in March 1971. The SJ-1 satellite served on orbit for over eight years, and was hailed for its breakthroughs in power, control, telemetry, and sensors.[42] Three ELINT satellites were launched as part of a follow-on "technical experiment satellite" series from July 1975 to August 1976.[43] These satellites were launched aboard the Feng bao-1 "Storm-1" launch vehicle which was specifically designed to meet the various requirements of ELINT satellite platforms.[44] In September 1981, China achieved a significant breakthrough, launching three Shijian-2 satellites aboard one carrier rocket, something observers saw as further adding to its ELINT satellite portfolio.[45] However, the initial high level Party leadership interest in the ELINT programme waned and nearly a decade followed with no known follow-on capability being launched.[46]

SIGINT sites for the collection of radio and Satellite Communication (SATCOM) are spread throughout China, with the net control station situated in Beijing. Outside China, a SIGINT station has been established on

40. Ibid., p.16
41. Ibid., pp.14-15.
42. SJ's "Scientific Exploration and Technological Experiment Satellite Series", *Huanqiu*, October 20, 2010, http://mil.huanqiu.com/weapon/2010-10/1185243.html.
43. "Imagery Reconnaissance and Electronic Reconnaissance Satellite Series", *Anhui News*, January 22, 2007, http://mil.anhuinews.com/system/2007/01/22/001656523.shtml
44. Mark A. Stokes, *China's Strategic Modernization: Implication for the United States* (Carlisle, PA: Strategic Studies Institute, 1999), p.4.
45. National Aeronautics and Space Administration (NASA), "Shijian 2B", National Space Science Data Centre, http://nssdc.gsfc.nasa.gov/nmc/masterCatalog.do?sc=1981-093A.
46. James A. Lewis, "China as a Military Space Competitor", Centre for Strategic and International Studies, August 2004, http://csis.org/files/media/csis/pubs/040801_china_space_competitor.pdf

Rocky Island (Shidao), near Woody Island in the Paracels. There have been persistent press reports of Chinese electronic surveillance sites in Myanmar, an ideal location for monitoring naval traffic in the Indian Ocean. China has also established multiple SIGINT sites in Myanmar and Laos. The Third Department and the Navy cooperate on shipborne intelligence collection platforms. Air force SIGINT collection is managed by the PLAAF Sixth Research Institute (*kongliusuo*) in Beijing.[47]

Building on the foundation established under the Shanghai Bureau of Astronautics' 701 Programme,[48] the People's Republic of China (PRC) appears to have resurrected efforts to develop and deploy a space-based ELINT capability as part of a broader surveillance and reconnaissance architecture for tracking and targeting US and allied maritime assets. ELINT technology is designed to intercept electromagnetic radiation, and works in tandem with imagery sensors – especially space-based Synthetic Aperture Radar (SAR) – for strategic and naval reconnaissance. China has long enjoyed Asia's most extensive SIGINT capability. However, most of its assets have been land-based and airborne, and not in space.[49] A surge of recent military space launches and a number of authoritative Chinese writings suggest that this may be changing. China has begun deploying a robust network of ELINT and imagery satellites in order to locate and track large warships, mobile air defence systems, and other critical defence systems.[50]

There have been numerous studies in China which have conducted evaluations on the effectiveness of a space-based information system in supporting ballistic missile operations and long-range precision strike.[51] For example, one study states:

47. Stokes,n.44, p. 34.
48. Ibid.
49. Lewis, n.46.
50. Easton and Stokes, n.7, p. 4.
51. Wu Weiqi and Zhang Yulin, "Effectiveness Evaluation Approach for Space-based Information Support System of Missile Operations", *Journal of the Academy of Equipment Command & Technology*, vol.17, no.2, 2006; Wu Weiqi and Zhang Yulin, "Space Information System Optimization for Long-range Precision Strike", *Journal of the Academy of Equipment Command & Technology*, vol.17, no.3, 2006.

Developments underway suggest that China is working to improve its ability to quickly download, process, and disseminate the intelligence gathered from space, including that from ELINT satellites.

> During the tactical process of ASBM attack/ defense the support of space-based satellite information is highly required for target reconnaissance, missile early-warning, global communications, precision guidance, battle damage assessment and the digitalized construction of the battlefield…Thus, an ASBM requires military satellite support at every stage of the attack process.[52]

In discussing the role that ELINT satellites would play in China's Anti-Ship Ballistic Missile (ASBM) programme, this study goes on to emphasise the importance of C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance) sensor fusion:

> During the process of planning [to use] the fire power of an ASBM, [there is a need] for obtaining reliable target intelligence information for guiding the missile attack. This could be achieved by integrating EO imaging satellites, SAR imaging satellites, electronic reconnaissance satellites, naval ocean surveillance system satellites, mapping resource satellites, and highly accurate commercial remote sensing satellite imagery, which could be purchased on the international market. Through the integration of the data obtained via a number of different satellites, and with the addition of processing and data fusion, [one could] guarantee missile guidance requirements for all types of target information for a long-range ASBM strike.[53]

This highlights the importance of developing a robust ground-based satellite support system to help integrate space-based ELINT into a broader

52. Pan Changpeng, Gu Wenjin and Chen Jie, "An Analysis on the Capabilities of Military Satellites to Support an ASBM in Offense and Defense Operations", *Winged Missiles Journal*, 2006, no.5, p.12.
53. Ibid., p.13.

C4ISR system. It also underscores the challenges in prioritising missions as the demand for ELINT collection capabilities comes from an expanding number of intelligence consumers. Authoritative sources suggest that China has made considerable progress in this area.[54]

Developments underway suggest that China is working to improve its ability to quickly download, process, and disseminate the intelligence gathered from space, including that from ELINT satellites. One study described the developments as such:

It appears that China is laying the foundation for what could be a robust space-based network of satellites dedicated to ELINT collection. It could also be developing clandestine piggy-backed sensors that could work with other space and terrestrially-based Intelligence, Surviellance, Reconnaissance (ISR) sensors to enable a truly informationalised network for global SIGINT/ELINT collection in near real-time.

> As electronic reconnaissance satellites develop, the requirement to obtain military intelligence from the satellites increases. The issue at hand is how to (from the ground) quickly, effectively set and decide satellite system mission tasking for effective, appropriate ground application of satellite resources… Satellite ground stations combine and use six systems for linking up with electronic reconnaissance satellite signals: 1) Antenna systems: responsible for uploading and downloading satellite signals; 2) Emitting systems: responsible for ordering satellite signal modulations, encryption, etc. Post-processing, these work through antenna systems; 3) Receiving systems: receiving signals from the satellites, and after processing then send to terminal station system; 4) Terminal station systems: responsible for reconnaissance data processing, satellite command and mission arrangement; 5) Monitoring and control systems: monitor satellites and downlink operation status and monitor over all ground station; 6) Power supply system: providing power for all ground station equipment. In short, an electronic reconnaissance

54. Stokes, p.44, p.8

satellite ground station is an integrated system for receiving, processing and managing data.[55]

China utilises shared facilities to support a number of satellites along with its maritime observation Haiyang series satellites. Ground stations supporting these satellites are located in Beijing, Sanya, Hangzhou, and Mudanjiang. China also has a ground station in Antarctica supporting these satellites.[56] It is reported to operate at least three other ground stations abroad. These are located in Swakopmund, Namibia; Malindi, Kenya; and Karachi, Pakistan.[57] China's operational headquarters and data processing centre for remote sensing satellites is located in Beijing, with three main ground stations supporting the network located in Miyun, near Beijing; Kashgar, in Xinjiang; and Sanya on Hainan Island.[58]

While it appears that China has experienced a lag in developing a robust electronic signals collection capability, there is another possibility one could posit. It is possible that the Chinese strategic leadership has long benefited from unidentified ELINT sensors attached to other satellite payloads, and recent launches simply represent an increase in dedicated systems. It is possible that SIGINT/ELINT sensors have piggy-backed aboard Chinese remote sensing satellites in Low Earth Orbit (LEO) and communications satellites in Geosynchronous Orbit (GEO) for many years.[59] Authoritative Chinese writings have explored the utility of GEO for SIGINT/ELINT sensors, stating:

55. Wang Lei, Zhou Qi, and Chen Peiqun, "LEO Electronic Reconnaissance Satellite Ground Station Mission Tasking and Decision-Making Methods", *Communication Countermeasures*, no.1, 2010, pp. 48-49; Wei Ping, "Architecture for Signal Processing Technology Used in Electronic Reconnaissance", *Communication Countermeasures*, vol.101, no.2, 2008, pp.3-7.
56. "Haiyang Satellite Ground Station Established in Antarctica", *Space Exploration*, no.1, 2010, p.12
57. Steven A. Smith, "Chinese Space Superiority? China's Military Space Capabilities and the Impact of Their Use in a Taiwan Conflict", *Air War College*, February 17, 2006, p.14, http://www.au.af.mil/au/awc/awcgate/awc/smith.pdf.
58. Evan Ellis, "Advances in China – Latin America Space Cooperation", *China Brief*, July 9, 2010, http://www.jamestown.org/single/?no_cache=1&tx_ttnews[tt_news]=36602&tx_ttnews[backPid]=13&cHash=23bb61c38d
59. Stokes, n.44, p. 10.

> In the information age, the utilization of electronic reconnaissance satellites to obtain intelligence has become an important method [of doing so]. Geostationary electronic reconnaissance satellites provide unique advantages and are being increasingly emphasized… Using geostationary satellite platforms to engage in electronic reconnaissance is useful for the large coverage ranges available for obtaining electronic information in the air, including terrestrial and other radar signals, communications signals, satellite telemetry, etc. It also allows for the continuous, long-term surveillance of target areas; obtaining intelligence in real-time to provide rapid electronic intelligence for diplomatic and strategic military decisions.[60]

In what could have implications for the clandestine use of telecommunications satellites in geostationary orbits for SIGINT/ELINT purposes, one Chinese aerospace electronics engineer at a research institute closely associated with the Chinese military analysed the use of airborne telecommunications systems for the collection of SIGINT, and found it to be possible to combine both the telecommunications and SIGINT missions on one hardware platform.[61]

Ultimately, Chinese writings advocate combining sensors in both orbital realms to optimise effectiveness.[62] It appears that China is laying the foundation for what could be a robust space-based network of satellites dedicated to ELINT collection. It could also be developing clandestine piggy-backed sensors that could work with other space and terrestrially-based Intelligence, Surviellance, Reconnaissance (ISR) sensors to enable a truly informationalised network for global SIGINT/ELINT collection in near real-time. This development may hold serious implications for the Asia-Pacific region, especially for major world powers as well as all

60. Dong Qiaozhong and Zhu Weiqiang, "Research on ELINT Satellite Techniques in GSO", *Electronic Warfare*, July 30, 2009, p.13.
61. Mao Cheng, "Design of RF Receiver System for Multi-Mission Payload, Telecommunications Engineering, July 2009, p.68.
62. Lu An'nan, "Thoughts on Developmental Problems of ELINT Satellite Passive Geo-location Techniques", *Communications Countermeasures*, March 2008, pp. 19-20.

international and regional actors' naval and air operations, air defence systems, communications security, counter-space requirements, and nuclear deterrence.[63]

As per the "2018 Worldwide Threat Assessment of the US Intelligence Community", released in February 2018, by the Office of the Director of National Intelligence, "If a future conflict were to occur involving Russia or China, either country would justify attacks against US and allied satellites as necessary to offset any perceived US military advantage derived from military, civil or commercial space systems".[64]

As per a RAND report, the role of the Strategic Support Force (SSF) also remains important, which is basically the infrastructure to support the PLA in the battlefield so that the PLA can achieve superiority in the space, cyber space, and all other electromagnetic domains. It is an important force in joint operations whose actions are integrated with the army, navy, air force, and rocket force.[65] Space-related units in the Space Systems Department include launch centres and satellite control centres from the former General Armament Department (GAD). Other units within the SSF include research institutes from the former General Staff Department (GSD)[66] and could also include units from the Third and Fourth Departments of the former GSD responsible for signals intelligence and electronic counter-measures and radar, respectively, as well as the Informatisation Department, which is responsible for communications.[67]

The SSF fulfills its space mission role in two ways. The first and main function of the SSF in regard to space is C4ISR support to an operational

63. Stokes, n.44, p. 14.
64. Statement for the Record Worldwide Threat Assessment of the US Intelligence Community, February 13, 2018, p. 13
65. Qiu Yue, "Our Military's Strategic Support Force Is What Type of Military Force?" (□军战略支援部队是一支□么样的军事力量？), China Military Online (□□军网), January 5, 2016.
66. "China PLA Strategic Support Force Network Systems Department 56th Research Institute" (中国人民解放军战 略支援部队网络系统部第五十六研究所), China Graduate Student Enrollment Information Network, May 24, 2017; and "China PLA GSD 58th Research Institute (中国人民解放军总参第五十八研究所), China Graduate Student Enrollment Information Network, September 13, 2016.
67. "Laser Ranging Systems Project Sole Source Announcement (激光探测定位系统项目单一来源采购公示公告),Beijing Guotai Jianzhong Management and Consulting Co. Ltd., October 31, 2016.

force through its computer network, communications, and space-operations functions. The SSF's C4ISR capabilities provide the connective tissue between units that enables the PLA to effectively conduct joint operations and successfully prosecute "system vs. system warfare" that the PLA characterises as essential to winning modern wars. The SSF fulfills this role by launching and operating China's satellite architecture, although its role in providing mobile space launch capabilities remains unclear. With its capabilities, the SSF plays a critical role in supporting the types of aerospace power projection operations the PLA expects it will need to conduct in future scenarios.[68]

Another important space function is the counter-space mission. Although information on this issue remains incomplete, the SSF's Space Systems Department appears to be charged with carrying out the co-orbital counter-space mission involving satellite-on-satellite attacks. It could logically be expected to take on responsibility for other counter-space missions as well, although Chinese publications provide little information on direct-ascent Anti-Satellite (ASAT) and directed-energy weapons capabilities due to the secretive nature of China's counter-space programme.[69]

Other counter-space functions performed by the SSF appear to be carried out by its Network Systems Department, which appears to be responsible for jamming satellite communications and Global Positioning System (GPS) signals, as well as hacking into the computer systems of space facilities and their satellites. The main direct war-fighting role of the SSF overall appears to be in the cyber and electromagnetic domains (a role that is beyond the scope of this paper). As a result, the SSF appears to be an organisational response to the PLA concept of integrated-network EW that emphasises combining cyber and EW forces into a joint force.[70] Additionally, because PLA strategists view space and cyber warfare as

68. Kevin L. Pollpeter, Michael S. Chase and Eric Heginbotham, "The Creation of the PLA Strategic Support Force and its Implications for Chinese Military Space Operations", *RAND*, RR2058, 2017.
69. Ibid.
70. Kevin L. Pollpeter, "Controlling the Information Domain: Space, Cyber, and Electronic Warfare," in Ashley Tellis and Travis Tanner, eds., *Strategic Asia: 2012-13: China's Military Challenge* (Seattle, Wash.: National Bureau of Asian Research, 2012), pp. 181-182.

important components of strategic deterrence alongside nuclear and conventional forces, the SSF would also appear to be poised to play an important role in China's further development of its strategic deterrence posture and in the conduct of deterrence operations.[71]

Many unknowns remain but there are strong indications that Chinese military and satellite intelligence is making up for the lack in matching up with the conventional forces that major world powers possess, redrawing geopolitical and geostrategic maps in South Asia, Southeast Asia and Central Asia, and strengthening the defensive as well as offensive capabilities for any future conflict that might force China to be a major player.

71. Pollpeter, et.al., n.68.