



## Current Structure of PRC Intelligence Services

### GUIDE TO THE STUDY OF INTELLIGENCE

## Chinese Intelligence

by Stefania Paladini, PhD

### Intelligence With Chinese Characteristics

Comparing systems and concepts like the Chinese and the Anglo-American is challenging, and intelligence studies are no exception. It is even more difficult, considering that there is not a perfect translation in Chinese for the word “intelligence.” In fact, the term used by the Chinese is *qingbao*, which can be translated as “information,” as much as “intelligence.” The Western distinction that intelligence is information that has been analyzed does not completely apply to Chinese doctrine. However, what is clear from Chinese terminology is the action-enabling purpose of intelligence – expressed with the terms *jihuo zhishi* – “activating knowledge.”<sup>1</sup>

Albeit this terminology-related question, China has a long tradition in this subject, and every cultivated Chinese, let alone politician and intelligence expert, knows about Sun Zi, the scholar from 300 BC who first theorized the use of intelligence, more specifically espionage, for warfare purposes.<sup>2</sup>

This article presents a brief overview of the intelligence organizations in the People’s Republic of China (PRC) and a few notes to understand intelligence with Chinese characteristics.<sup>3</sup>

1. There is also another term used, *ziliao*, which refers to data, and often is put in comparison with *qingbao*, which generally involves an element of secrecy. For more about this linguistic debate, see Huo & Wang, 1991, and Mattis, 2013 in the “Readings for Instructors” section.

2. Sun Zi is often Romanized as Sun Tzu.

3. This article does not address Taiwan, Hong Kong, or Macao. While

There are several intelligence and security organizations in the PRC, some part of larger organizations. None is in charge overall. Only the ones exclusively devoted to intelligence are presented here, and the list is not exhaustive.<sup>4</sup> Furthermore, a section intentionally missing here regards the important area of intelligence oversight. This is because intelligence activities in China lack parliament oversight for the basic reasons that China is not a democracy (apart from direct elections at township and local level) and there are not transparent rules to how security, internal and external, is ensured.

The obvious starting point is the **Ministry of State Security** (Guójiā Ānquánbù, 国家安全部, MSS). It is the main agency, responsible for intelligence and state security, in charge of counterintelligence and foreign intelligence (but not military intelligence). It was established in 1983, with Ling Yun as first chief, after the reform of the predecessor Central Investigation Department (Diaochabu) that was established at the creation of PRC in 1949 and first headed by Kang Sheng and later by Li Kenong. Before that there was no intelligence service separate from the Communist Party, even though there were organized intelligence activities since at least 1927.

According to the Federation of American Scientists,<sup>5</sup> the MSS is organized – unsurprisingly – on the model of the old KGB, with a First Bureau dealing with domestic security, the Second with foreign services and counterintelligence. Other sections deal with signals intelligence (SIGINT) and countersurveillance, or focus on outer territories like Taiwan. According to some sources, the 17th Bureau is in charge of economic intelligence, the collection of which is one of the characteristics of Chinese services, which have targeted specifically the United States and European countries, France among them.

considered part of Chinese territory by the PRC Government, the first is labeled a “renegade province” and the other two go under the term of “one-country, two systems.”

4. One of the best open sources is the French intelligence service website: <http://servicederenseignements.e-monsite.com/pages/grandes-agences/republique-populaire-de-chine.html>. French sources are especially good concerning Chinese intelligence, starting with Faligot & Remi (1990), which is a recommended reading.

5. FAS’ own source here is: “Spy Headquarters Behind the Shrubs — Supplement to ‘Secrets About CPC Spies’” No. 233, by Tan Po Cheng Ming [Hong Kong], March 1, 1997, 34-37; Cheng Ming on Chinese Spy Headquarters, FBIS-CHI-97-047, March 1, 1997. Source no longer retrievable.

French sources<sup>6</sup> in 2005 estimated the MSS had around 7,000 employees, but some 50,000 undercover operatives.<sup>7</sup> The chief of the service, since early 2015, is Geng Huichang. According to many observers, he is President Xi Jinping's man and not a holder of autonomous power, as often has been the case with former chiefs.

The MSS should not to be confused with the **Ministry of Public Security** (Gōng'ānbù, 公安部, MPS) that looks after the police bureau and internal/ordinary security,<sup>8</sup> but has no intelligence gathering mission.<sup>9</sup>

Military intelligence is the prerogative of the People's Liberation Army (PLA). Two PLA departments specifically deal with it:

One is the **PLA General Staff Headquarters Second Department (Qingbaobu, 2PLA)**, which is more specifically responsible for collecting and disseminating military information, via human sources (HUMINT), signals intelligence (SIGINT), and imagery intelligence (IMINT). Officers are dispatched to China's embassies and consulates overseas, and also to big Chinese state-owned enterprises (SOEs), banks, and think tanks. On the other hand, the **Third Department (3PLA)** is in charge of the direct monitoring of foreign armies and their SIGINT, and with dissemination of collected intelligence. It should be mentioned that Chinese SIGINT is quite impressive and is considered the most extensive of all Asian countries.

2PLA also has a military counterintelligence service called **Chi Pao Ko**,<sup>10</sup> which exercises a degree of influence on think tanks and research institutes connected with intelligence studies in China, such as the China Institutes of Contemporary International Relations (CICIR, primarily connected to the MSS) and the China Institute for International Strategic Studies (CISS).<sup>11</sup>

There are other bodies in China performing specific kinds of intelligence activities, but they are less prominent than the ones presented here.

Worth mentioning are a couple of historical notes on Chinese intelligence. Sun Zi's *Art of War*, the classical text about military strategy from the fifth century

BC, devotes the last chapter to intelligence and is still a most common reference about the practice and doctrine of espionage and its political uses.<sup>12</sup> Intelligence operations in Communist China started long before 1949 and are linked to Kang Sheng,<sup>13</sup> Mao Zedong's spymaster and a central figure in China's foreign policy for decades. Among other achievements, Kang Sheng played a substantial role in obtaining nuclear technology for developing a national atomic program.

Another figure to be mentioned for importance is the second MSS chief. Soon after the removal of its first chief, Lin Yun, in 1985 over the defection of Yu Qiangsheng, head of the Counterespionage Bureau, to the US, Jia Chunwang rose to power and held tenure until 1998; until today the longest serving MSS chief and one of the most influential. Jia's tenure was fundamental in expanding the MSS' scope and grasp of the MSS.<sup>14</sup> The MSS began as a central-level ministry with only a handful of provincial departments. By the end of Jia's tenure, the MSS covered every province, provincial-level city, and a countless number of municipalities.

## Chinese Methods and Approach to Intelligence

The methods used by Chinese intelligence often differ from the more easily understood methods of other nations. Not only does the collection of intelligence present some peculiarities, as outlined below, but Chinese methods have evolved considerably over the years.

In the 1950s and 1960s, every Chinese diplomatic post overseas had an Investigation and Research Office with staff from the Central Investigation Department—the so-called Institute of Contemporary International Relations. However, from Deng Xiaoping (in office from 1981 to 1989) onward, non-intelligence personnel, from newsmen to businessmen to academic researchers, started to be charged with intelligence collection tasks. Only a few career officers were left in embassies.

6. French intelligence website, accessed on March 2015.

7. In MSS slang, the often dormant, long-term operatives are called "fish at the bottom of the ocean" (*Chen di yu*). Eftimiades, 1999, 35.

8. An important exception here is riot control, which is not under MPS domain but is taken care of by the Chinese People's Armed Police Force (中国人民武装警察部队, CAPF) at the provincial level.

9. The two services are located near each other at 14, Dongchang'an (East Chang'an Street), Beijing.

10. Belonging to PLA Intelligence is Xiong Guangkai, considered by many the most important intelligence figure of the last two decades (Mulvenon, 2008).

11. See Gates & Mulvenon, 2002

12. "What enables the wise sovereign and the good general to strike and conquer, and achieve things beyond the reach of ordinary men, is foreknowledge. Now this foreknowledge cannot be elicited from spirits; it cannot be obtained inductively from experience, nor by any deductive calculation. Knowledge of the enemy's dispositions can only be obtained from other men" (Sun Zi, *The Art of War*, Chapter 13).

13. Given that this brief outline excludes Taiwan, all references to Chiang Kai-shek (Jiang Jieshi) and his formidable intelligence apparatus have been omitted. However, it is worth noting that Tai Li (Dai Li), his intelligence chief, was for many years a valid adversary to Kang Sheng. For more about Dai Li, see the recommended readings.

14. Mattis, 2011.

In general, Western perceptions of Chinese intelligence have long been biased due to the fact that China is essentially an inward-focused country. When it comes to security, its approach to intelligence gathering has been often regarded as “unsophisticated and risk-averse, particularly when you consider the bureaucratic inefficiencies inherent in the Communist Party of China’s (CPC) administrative structure. But it is an approach that takes a long and wide view, and it is more effective than it may seem at first glance.”<sup>15</sup> There are at least the three main Chinese intelligence-gathering characteristics, which often overlap, and that make China’s approach to intelligence and espionage different.

Most important is the so-called mosaic approach, where low-grade and generally unclassified, but massive in scope, information is collected by thousands of assets. According to the open-source intelligence company Stratfor, this approach is particularly successful because it is designed to “overload foreign counterintelligence agencies by the painstaking collection of many small pieces of intelligence that make sense only in the aggregate. This is a slow and tedious process, and it 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.”<sup>16</sup>

Another important characteristic is related to the identity of the intelligence collectors. Most of the time, they are not professionals, but amateurs recruited among Chinese-born residents in other countries or students and researchers who are abroad for study and research.<sup>17</sup>

The third method is the long-term cultivation of foreign assets, often via blackmail, honey-pots,<sup>18</sup>

corruption, or other expedients, once useful pressure points of the targets are identified.

Surprisingly enough, given this highly specific approach, Chinese doctrine is more similar to Western approaches than one might imagine. This is evident looking at scholarly articles on the subject, especially recent ones. This is due to the fact that Chinese doctrine has evolved considerably over the years, mirroring the progressive opening of China to the Western world and the increasing amount of knowledge available. As one of the most prominent scholars of Chinese intelligence has written, “Chinese writings on intelligence bear remarkable similarity to familiar US definitions of intelligence functions and goals.”<sup>19</sup>

Finally, in the last 20 years, new methods for intelligence collection have emerged in the cyber world.

### Some Case Studies

Since 2003, 123 Chinese agents have been identified in the US.<sup>20</sup> It is impossible to present here, even briefly, all instances of Chinese espionage over the decades. Some cases, however, stand out.

One of the most damaging was Larry Wu-Tai Chin who worked for the US Army as a translator beginning in 1944. After becoming an American citizen, he worked for the Central Intelligence Agency’s Foreign Broadcast Information Service (FBIS). For decades until his apprehension in 1985, he spied on the US and “revealed President Nixon’s desire to open diplomatic relations two years before the policy was implemented.”<sup>21</sup>

A substantial focus of Chinese activities targeted US military secrets, especially nuclear technology. A most important analysis is the 1988 *Report of the Select Committee on US National Security and Military/Commercial Concerns with the People’s Republic of China*, US House of Representatives (Cox Report), released in redacted form during the Clinton Administration in the 1990s. While some parts of the report remain classified, the report stated that China had managed to obtain sensitive information about thermonuclear weapons, including deployment details and reentry vehicles. An FBI investigation, codenamed Kindred Spirit, took place when “US intelligence discovered in 1995 that secrets about the W88, the most advanced miniature

15. Stratfor, 2010.

16. *Guanxi* is a typical feature of the Chinese culture, and it can be translated as “network.” (Stratfor, 2010, 2). But *guanxi* also means “relationships” and is “a system of interpersonal relationships that has long historical and cultural roots,” constituting an essential feature of Chinese society. “*Guanxi* itself works as an important power base that represents saved favors, faces, and special relationships with powerful people. When relational norms and Confucian values are considerably eroded, *guanxi* could bring out further egoism, opportunism, and instrumentality” (Y. Luo, “The changing Chinese culture and business behavior: The perspective of intertwinement between *guanxi* and corruption,” *International Business Review* 17 (2), 2008, 188-193.

17. The closest equivalent practice is by Israel’s Mossad, which employs the Sayanim, volunteers in the Jewish diaspora not directly connected with the intelligence services but willing to help and provide various services.

18. A few instances have been recorded. One of the most famous was the Bernard Boursicot case, a French diplomat caught in Kang Sheng’s net in the 1970s when he became enamored of a Beijing transvestite opera singer, Shi Peipu.

19. Mattis, 2012:3.

20. Ibid. This number is as of April 2015.

21. David Major and Peter Oleson, “Espionage Against America,” *Guide to the Study of Intelligence*, Association of Former Intelligence Officers, <http://www.afio.com/publications/MAJOR%20OLESON%20Espionage%20Against%20America%20DRAFT2%202015Aug31.pdf>.

nuclear warhead (deployed on the Trident II SLBM), may have leaked from Los Alamos National Laboratory to China between 1984 and 1988. US intelligence reportedly was handed a secret PRC document from 1988 containing designs similar to that of the W88.”<sup>22</sup>

The Cox Report warned that “elements of the stolen information on US thermonuclear warhead designs will assist the PRC in building its next generation of mobile ICBMs” and, more worryingly, that “despite repeated PRC thefts of the most sophisticated US nuclear weapons technology, security at our national nuclear weapons laboratories does not meet even minimal standards.”<sup>23</sup> Subsequent investigations focused on three Chinese-Americans, Guo Bao Min, employed at Lawrence Livermore National Laboratory; Wen Ho Lee, on the staff of Los Alamos National Laboratory where the W-88 warhead was designed; and Peter Lee, also at Los Alamos and TRW Corporation.

Another famous case was Chi Mak, an “illegal” sleeper agent sent to the US to gain access over the long term to US military technologies, and the object of one of the FBI’s biggest counterintelligence operations. He managed to send to China information on sensitive electric drive technology for submarines. On May 10, 2007, a jury convicted Mak on charges of conspiring to export US military technology to China and acting as an unregistered agent of a foreign government.<sup>24</sup>

But Chinese intelligence activities have not just targeted military objectives. For instance, a lot of press attention has been given to Katrina Leung, the lover of two FBI counterintelligence special agents focused on Chinese intelligence activities who had initially recruited her as an asset. She was in reality an MSS double agent and managed since 1991 to pass classified information to the Chinese Government.<sup>25</sup>

A growing number of cases are concerned with industrial espionage. According to FBI data, since 2006,<sup>26</sup> there have been federal investigations and

criminal prosecutions of about 44 individuals in 26 separate investigations.

An example is the case of Dongfan Chung, a Chinese-born naturalized American and an engineer working at Rockwell International and Boeing. As a result of his activities, an impressive amount of technological details was revealed regarding the B-1 bomber, Delta IV space launch vehicle, the C-17 cargo plane, the F-15 fighter, and, last but not least, the Space Shuttle. He was sentenced to 15 years in prison for economic espionage.

The outlook will not be complete without briefly mentioning the so-called 863 Program sponsored since 1986 by the PRC’s State High Technology R&D Organization, i.e. a specific kind of approach where companies steal US commercial technologies to advance the Chinese economy.<sup>27</sup>

## Chinese Cyber Activities

Chinese cyber espionage represents a substantial threat to Western countries. It long has been known that China uses state-sponsored “hackers.” Also, the PLA has a military espionage unit specifically devoted to cyber operations, the Chengdu Province First Technical Reconnaissance Bureau (TRB).<sup>28</sup>

According to the Cyber Intelligence Sharing and Protection Act (CISPA), “China is the world’s most active and persistent perpetrator of cyber economic espionage. US companies have reported an onslaught of Chinese cyber intrusions that steal sensitive information like client lists, merger and acquisition data, pricing information, and the results of research and development. This illegally-acquired information gives Chinese companies an unfair competitive advantage against the companies from which it was stolen.”<sup>29</sup>

The most famous instance to date has been the 2010 attack on Google servers, which were attacked in “a concerted political and corporate espionage effort that exploited security flaws in e-mail attachments to sneak into the networks of major financial, defense and technology companies and research institutions in the United States.”<sup>30</sup> With Google, about 20 other companies, such as Yahoo, Symantec, Adobe, and

22. (Kan, 2006, 5).

23. The tone, if not the conclusions of the Cox Report, has been criticized by a group of scholars from Stanford University, which observed in a note that “The language of the report, particularly its Overview, was inflammatory and some allegations did not seem to be well supported.” The details of the Stanford note have been provided in the reference list for documentation, while the debate about the report remains open.

24. Yudhijit Bhattacharjee, 2014 “How the F.B.I. Cracked a Chinese Spy Ring,” *The New Yorker*. May 12, 2014. Available at: <http://www.newyorker.com/news/news-desk/how-the-f-b-i-cracked-a-chinese-spy-ring>. [Accessed 15 Jun. 2015].

25. Lloyd Vries, “Real-Life ‘Spy Who Loved Me’ Scandal,” CBS News, April 16, 2003. Available at: <http://www.cbsnews.com/news/real-life-spy-who-loved-me-scandal/> [Accessed 15 Jun. 2015].

26. I. C. Smith & Nigel West, *Historical Dictionary of Chinese Intelligence* (Lanham, MD: The Scarecrow Press, 2012).

27. Among the most-sought after sectors are biotechnologies, space, IT, and energy; while, geographically speaking, California’s Silicon Valley is the main target.

28. Wise, 2011.

29. CISPA, 2012.

30. Ariana Eunjung Cha and Ellen Nakashima, “Google China cyberattack part of vast espionage campaign,” *Washington Post*, January 14, 2010. <http://www.washingtonpost.com/wp-dyn/content/article/2010/01/13/AR2010011300359.html?sid=ST2010011300360>.

Northrop Grumman, have found that Chinese hackers targeted them, in what has been dubbed “Operation Aurora.”<sup>31</sup>

However, it would be incorrect to believe that only government-sponsored espionage exists. As the Cox Report clarified, a plethora of Chinese actors – public and private – have been involved in technology theft and economic espionage. There have been, for example, cases involving Chinese corporations as well – with the result that some of them have been denied the acquisition of American companies and their technologies, for example Huawei and ZTE. In both cases, the companies have been excluded in the US (and Huawei later in Canada) from public works on the basis of national security. The companies, on the other hand, have always maintained they were private corporations, with no links or instructions from the Chinese Government to illegally acquire Western technology.<sup>32</sup>

### Recent Developments

Another important point is how the system regulates itself from within. What is evident is that every change in CPC leadership – at this moment with the fifth generation leaders at the helm since the November 2012 18th Party Congress – is normally carried along with some purges at the top of those services. This is what has happened with the new leader, Xi Jinping, CPC general secretary and PRC president, and the procedures still appear to be ongoing at the moment.

As a matter of fact, since 2013, Xi has been waging an anti-corruption campaign that is considered by many observers as a way to get rid of political adversaries, in the biggest purge since the Cultural Revolution (around 15,000 people to be investigated). One of the latest victims has been, in January 2015, Vice Minister Ma Jiang,<sup>33</sup> MSS chief, implicated in the Founder Group’s investigation.<sup>34</sup> Ma was a high-pro-

file official, in charge of China’s counterespionage operations, and the highest-ranking security official investigated after Zhu Yongkang, MPS chief between 2002-2007.<sup>35</sup> Zhu was demoted in July 2014. He was the first member of the Politburo’s Standing Committee to be involved in an official investigation in the PRC’s history. While the official charges, which were formalized in April 2015, talk of “bribes, abuse of power and intentionally leaking state secrets” that cover a period since 1988, thus most of Zhu’s three-decade political career, the outlook seems more complex than that. As related by the *South China Morning Post*, “The Supreme People’s Court said last month that Zhou had ‘undermined the party’s solidarity and engaged in political activities not approved by the authorities,’ a rare accusation that some analysts suggested was an indication that Zhou would face charges for political offences.” The trial, held in Tianjin No. 1 Intermediate People’s Court in spring 2015, where Zhou risked a death penalty, concluded in June 2015 with the former security czar pleading guilty and receiving a sentence of life imprisonment.<sup>36</sup>

### Readings for Instructors

There are a few important on-line references for Chinese intelligence services, although some are not up-to-date. They still represent a useful starting point for instructors. The main three to be consulted are:

- <http://www.globalsecurity.org/intell/world/china/mss.htm>.
- <http://fas.org/irp/world/china/mss/index.html>.
- <http://servicederenseignements.e-monsite.com/pages/grandes-agences/republique-populaire-de-chine.html>.

Also, there are the websites of Chinese think tanks devoted to, among other subjects, intelligence

31. Ibid.

32. Ellen Messmer, “A House Intelligence Committee report blasts Huawei and ZTE as threats to U.S. national security,” *NetworkWorld*, October 8, 2012. Available at: <http://www.networkworld.com/article/2160516/data-center/house-intelligence-committee-report-blasts-huawei-zte-as-threats-to-u-s-national-secur.html>.

33. Jamil Anderlini, “Chinese spymaster Ma Jian detained in corruption purge,” *Financial Times*, January 12, 2015. <http://www.ft.com/cms/s/0/84707fd8-9a37-11e4-8426-00144feabdc0.html#axzz3O-d8O0tbm>

34. Founder Group is a Beijing University-owned technology company, under investigation since 2012 over corruption claims. “Founder has been involved in a high-profile spat with Beijing Zenith, a property developer with a mysterious background, but which is also the second-biggest shareholder in the conglomerate’s Founder Securities unit. Beijing Zenith publicly accused Founder executives of insider trading and misappropriating company assets to the tune of several

billion yuan.” (2015). “Chinese spy chief Ma Jian detained as corruption crackdown widens.” *South China Morning Post*, January 11, 2015. Available at: <http://www.scmp.com/news/article/1678537/chinese-spy-chief-ma-jian-detained-corruption-crackdown> [Accessed 15 Jun. 2015].

35. Li Jing, “China’s ex-security chief Zhou Yongkang charged with corruption, leaking secrets,” *South China Morning Post*, April 3, 2015 [http://www.scmp.com/news/china/article/1755037/chinas-ex-security-tsar-zhou-yongkang-indicted-after-graft-probe?utm\\_source=edm&utm\\_medium=edm&utm\\_content=20150403&utm\\_campaign=breaking\\_news](http://www.scmp.com/news/china/article/1755037/chinas-ex-security-tsar-zhou-yongkang-indicted-after-graft-probe?utm_source=edm&utm_medium=edm&utm_content=20150403&utm_campaign=breaking_news).

36. Alvin Yibanez, “Ex-Security Chief Zhou Yongkang Sentenced to Life in Prison,” Yibada [online]. Available at: <http://en.yibada.com/articles/38175/20150613/ex-security-chief-zhou-yongkang-sentenced-life-prison.htm>. [Accessed 15 Jun. 2015]. Yet, “with the arrest of a major leader in a continuing, and massive, purge, and constant reminders that the stakes of the struggle against corruption are nothing less than the survival of the party, Xi and his colleagues have sought to generate a period of crisis in which major changes are possible. The question to remain is whether this political window is wide enough—and will stay open long enough—to allow systemic change to take root” (Cohen, 2014).

studies, some of them only available in Chinese. For an updated list of the most prominent of them and a brief description, see: <http://libguides.gwu.edu/content.php?pid=77975&sid=591628>.

### Recommended books and journal articles include:

- Bates, G. and J. Mulvenon, "Chinese Military-Related Think Tanks and Research Institutions," *The China Quarterly* 171, September 2002.
- Byron, J. and R. Pack. *The Claws of the Dragon: Kang Sheng-the Evil Genius Behind Mao and His Legacy of Terror in People's China* (New York: Simon and Schuster, 1992).
- Eftimiades, Nicholas. *Chinese Intelligence Operations* (Annapolis, MD: Naval Institute Press, 1994).
- Faligot, R., and K. Remi, *The Chinese Secret Service* (New York: William Morrow & Co., 1990).
- Huo, Z. & Z. Wang. *Techniques of Obtaining National Defense Science and Technology Intelligence*, [Guofang Keji Qingbaoyuan ji Huoqu Jishu] [Kexue Jishu] (Wenxuan Publishing Co., Beijing, 1991), available at: <http://fas.org/irp/world/china/docs/sources.html>.
- Lin, Q. *Kan Sheng Waizhuan [An Unofficial Biography of Kang Sheng]* (Beijing: Zhongguo Qingnian, 1988).
- Kan, Zhongguo, "Intelligence Agencies Exist in Great Numbers, Spies Are Present Everywhere; China's Major Intelligence Departments Fully Exposed," *Chien Shao* (Hong Kong, 1 January 2006).
- Kan, S. *China: Suspected Acquisition of U.S. Nuclear Weapon Secrets*, CRS Report for Congress, RL30143, 2006, online at: <https://www.fas.org/sgp/crs/nuke/RL30143.pdf>.
- Li, Mingyang, (ed.). *Sunzi Bingfa [SunTzu's Art of War]* (Hefei, Anhui: Huangshan Shushe, 2001).
- Mattis, P., "Assessing the Foreign Policy Influence of the Ministry of State Security," *China Brief* 11 (1), January 14, 2011.
- Mattis P., "The Analytic Challenge of Understanding Chinese Intelligence Service," *Studies in Intelligence* 56 (3), September 2012. Available at: <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol.-56-no.-3/pdfs/Mattis-Understanding%20Chinese%20Intel.pdf>.
- Roche, E. M. *Corporate spy: Industrial Espionage and Counterintelligence in the Multinational Enterprise* (New York: Barraclough, 2008).
- Smith, I. C. and Nigel West, *Historical Dictionary of Chinese Intelligence* (Lanham, MD: The Scarecrow Press, 2012).
- Stokes, M., J. Lin, and L.C. Russell Hsiao, "The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure," *Occasional Paper*, Project 2049 Institute, 11 November 2011.
- Sun Zi, *The Art of War*, online at: <http://ctext.org/art-of-war>.
- Trulock, Notra. *Code Name Kindred Spirit: Inside the Chinese Nuclear Espionage Scandal* (San Francisco: Encounter Books, 2004).
- Wakeman, F. *Spymaster: Dai Li and the Chinese Secret Services* (Berkeley: University of California Press, 2003).

Wise, David. *Tiger Trap: America's Secret Spy War With China* (Boston: Houghton Mifflin Harcourt, 2011).

Zhang, Shaojun, et al. *Junshi Qingbao Xue [The Science of Military Intelligence]* (Beijing: Junshi kexue chubanshe [Academy of Military Science Press], 2001), 6, 10–12.

### Newsclippings and other media sources consulted for the writing of this article:

- Cohen, D., "Zhou's Fall About Institutions, Not Personalities," *China Brief* 14 (15), July 31, 2014. [http://www.jamestown.org/programs/chinabrief/single/?tx\\_ttnews%5Btt\\_news%5D=42688&tx\\_ttnews%5BbackPid%5D=758&no\\_cache=1#.VVJClpVikp](http://www.jamestown.org/programs/chinabrief/single/?tx_ttnews%5Btt_news%5D=42688&tx_ttnews%5BbackPid%5D=758&no_cache=1#.VVJClpVikp).
- deGraffenreid, Kenneth (ed.). *The Unanimous and Bipartisan Report of the House Select Committee on U.S. National Security and Military Commercial Concerns With the People's Republic of China ("The Cox Report")*. (Washington, DC: Regnery, 1999). A copy of the declassified sections of the Cox Report is accessible at: <http://www.house.gov/coxreport/chapfs/over.html>.
- Johnston, A. et al, "The Cox Committee Report: An Assessment," 1999, online at: <http://iis-db.stanford.edu/pubs/10331/cox.pdf>.
- Mattis, Peter, "Five Ways China Spies. Not as different as you might think," *National Interest*, March 6, 2014 at <http://nationalinterest.org/commentary/five-ways-china-spies-10008>.
- Lo, Ping, "Secrets About CPC Spies — Tens of Thousands of Them Scattered Over 170-Odd Cities Worldwide," *Hong Kong Cheng Ming* No. 231, 1 January 1997, 6-9 ["Journal Discloses 'Secrets' About PRC Spy Network," *FBIS-CHI-97-016*, 1 Jan 1997]. ✓

Dr. Stefania Paladini is an associate professor at Coventry University, UK, where she is also in charge of a EU-FP7 project researching Chinese investments in Europe. Before joining academia, she worked several years for the Italian government, seven of which were spent in East Asia as trade commissioner. She obtained her PhD in international relations and security studies from City University of Hong Kong.