‘The Enlightened Prince and the Wise General’

Hughes, Robert G.; Chen, Kai

Published in:
Intelligence and National Security

DOI:
10.1080/02684527.2018.1492890

Publication date:
2019

Citation for published version (APA):
Hughes, R. G., & Chen, K. (2019). ‘The Enlightened Prince and the Wise General’: The History of Chinese Intelligence. *Intelligence and National Security*, *34*(7), 1085-1091. https://doi.org/10.1080/02684527.2018.1492890

Review Article

The History of Chinese Intelligence

R. Gerald Hughes and Kai Chen

I.C. Smith and Nigel West, *Historical Dictionary of Chinese Intelligence* (Lanham, MD/Toronto/Plymouth, UK: The Scarecrow Press, 2012), pp. 392, hbk, US$110/£80. ISBN: 978-0810871748.

> '[T]he reason the enlightened prince and the wise general conquer the enemy whenever they move and their achievements surpass those of ordinary men is foreknowledge.' Sun Tzu[1]

The activities of Chinese intelligence agencies, like so many facets of that country, has long intrigued scholars and commentators in the West. In 2014 Peter Mattis, a then fellow of the Jamestown Foundation, noted the enduring 'mystique [that] surrounds Chinese intelligence.' It's not just that China is a rival and *the* global rising power. China has not been 'opened up' by the revelations that the Russians have endured through defectors (such as from Oleg Gordievsky, Vasili Mitrokhin, Sergei Tretyakov and others). Such sources account for our knowledge of Soviet era intelligence. Thus, with regard to the People's Republic, the continuing 'shroud of mystery has meant Western observers treat Chinese intelligence as a kind of inscrutable beast, operating in fundamentally different ways than their Western and Russian counterparts.'[2] New analyses are useful and, in this vein, the publication of this encyclopedic-type volume on the history of Chinese intelligence should be most welcome. It is certainly true that the *Historical Dictionary of Chinese Intelligence*, written by I.C. Smith (former FBI investigator working in Chinese counter-intelligence) and Nigel West (prolific author and the editor of the *International Journal of Intelligence and Counter-Intelligence*), digs deep into the dynamics of Chinese intelligence and counter-intelligence. And Chinese intelligence, like the Chinese state itself, has a long history (which can be tracked back all the way to the timeless *The Art of War* by Sun Tzu).

In his review in the CIA in-house journal, *Studies in Intelligence*, Peter Mattis notes that Smith and West mistakenly assert that 'In the Chinese language, there is no real distinction between 'intelligence' and 'information' in common usage.' (p. 220). In fact, 'intelligence' as rendered in Chinese implies information that is actionable. As early as 1915, the standard scholarly dictionary (*Cihai*) defined 'intelligence' as being 'wartime reports on the adversary's condition'. The wrongheaded rendering of

[1] Sun Tzu, *The Art of War* (Oxford: Oxford University Press, 1963), p. 144.

[2] Peter Mattis, 'Five Ways China Spies', *The National Interest*, 6 March 2014.

'intelligence' as 'information' then leads the authors to construct the case that Chinese intelligence processes and institutions are fundamentally distinct from the Western and Russian models (pp. 3-11).[3] Amongst scholars, 'mirror-imaging' has long been a popular criticism of policymakers and intelligence agencies but the assumptions made by Smith and West originate from a similar thought process.

Although many in the West expend a good deal of effort seeking to understand Chinese intelligence, basic erroneous assumptions distort conclusions. The near-obsessive focus with intuitions, has all too often led to a belief that 'Chinese intelligence agencies' produce 'Chinese intelligence'. It is assumed that the People's Republic of China operates a strongly centralised and monolithic model when it comes to gathering intelligence. This arises out of an assumption that the PRC is possessed of a structure akin to that prevailing in the Soviet Union during the Cold War (or similar). In a recent review, Sergey Radchenko criticised a particular book on Chinese intelligence for its lack of context – especially the political context within which 'intelligence' operates. (And in pursuing this end, the close study of Chinese 'strategic culture'[4] would yield commensurate benefits).[5] The book under review, Radchenko contends, thus concentrates on bodies like the Ministry of Public Security and the nature of the information that it actually collects, whilst engaging in an all-too-brief discussion of how Chairman Mao Zedong 'perceived the role of intelligence'.[6] Taking us back to the basics of intelligence gathering, Peter Mattis reminds us of five ways in which the PRC gathers intelligence outside of the familiar intelligence structures of the modern national security state.[7]

- Diplomats, defence attachés and journalists
- Seeding Operations (i.e. penetrating the adversary's structures)
- Academics and scholars
- The cover afforded by local government offices in the PRC
- Businesspersons in the PRC itself and overseas

In part, at least, such misperceptions of China (and, indeed, of many states' manner of utilising intelligence) are derived from the fact that it is all too often forgotten that *intelligence* is partly comprised of *information*. Intelligence is not (or at least not always) information derived from the clandestine activities of intelligence agencies. This is a crucial point. The notion that all intelligence is clandestine and all intelligence is gathered by dedicated collection bodies is all too prevalent amongst even those who really should know better. (And, of course, intelligence agencies and

[3] Peter Mattis, review of I.C. Smith and Nigel West, *Historical Dictionary of Chinese Intelligence* in *Studies in Intelligence*, 56/4 (2012), p. 23.
[4] On this specifically, see Warren I. Cohen, 'China's Strategic Culture', *Atlantic Monthly*, 279/3 (1997), pp. 103-5.
[5] See, for example, Xuezhi Guo, *China's Security State: Philosophy, Evolution and Politics* (Cambridge: Cambridge University Press, 2012).
[6] Sergey Radchenko, review of Michael Schoenhals, *Spying for the people: Mao's secret agents, 1949–1967*, *Intelligence and National Security*, 31/6 (2016), p. 929.
[7] Mattis, 'Five Ways China Spies'.

their employees are all too keen to perpetuate the myth of the omnipotence of intelligence agencies). It is important to remember that the effective use of intelligence for many states predated the establishment of the formal administrative bodies with a remit to 'do' intelligence. The British, for example, had a reputation for effective collection and use of intelligence long before the establishment of the Secret Intelligence Service (SIS) in 1909. Clumsy assumptions continue to cause problems for those seeking to further our understanding of Chinese intelligence.

> One of the reasons Chinese intelligence operations do not seem to make sense to observers is that they mistake intelligence for the theft of secrets. Intelligence does not mean the acquisition of "classified" or "secret" information. Intelligence is the acquisition and processing of information that assists in formulating policy and guiding action. Classification has nothing to do with it; Beijing's concerns do. China concerns in the United States go beyond U.S. policy, including overseas Chinese populations, democracy activists, counterintelligence, and scientific expertise. And … the Chinese seem to be very comfortable with merely secondhand access to sensitive information.[8]

The wrongheaded nature of certain of the external views of the intelligence cycle in China notwithstanding this volume is still of value (not least die tot the fact that such misperceptions are applied to a great many states). This dictionary is thus to be welcomed for the manner in which it meticulously explores and analyses numerous cases regarding Chinese intelligence and counter-intelligence over an extended historical span. Many of the cases and concepts under discussion in this volume demonstrate nothing so much as the fact that, in the main, the Chinese experience of intelligence is different from those of their Western counterparts. The authors deploy comprehensive cross-references, making this volume more readable and more useful to readers with an interest in the burgeoning field of Chinese Intelligence Studies.[9] The volume is sub-divided into three sections. First, we are presented with a chronology of Chinese intelligence. Second, the authors seek to outline the evolution and development of Chinese intelligence operations. And, third, the dictionary itself. This is by far the longest portion of the book and contains a myriad of entries (many of which have, alas, only a tangential relationship with Chinese intelligence *per se* – e.g. Uzbekistan (p. 278)).

To a Chinese reviewer in particular, this dictionary makes two central contributions to the literature on Chinese intelligence and counter-intelligence. First, although many cases of US intelligence and counter-intelligence activities against the People's

[8] Mattis, 'Five Ways China Spies'.

[9] On this, see the recent piece in the CIA in-house journal, namely: David Ian Chambers, 'Edging in from the Cold: The Past and Present State of Chinese Intelligence Historiography', *Studies in Intelligence*, 56/3 (2012), pp. 31-46.

Republic of China are well documented, many of these cases are still not familiar to Chinese readers. To take one example, the authors record the fact that, in 1981, a former US marine, one Lawrence Gardella, published a sensational memoir entitled *Sing a Song to Jenny Next*. This book 'revealed' a top-secret US mission into the People's Republic of China and, as an adventure yarn, it rivalled the likes of Fitzroy Maclean. The mission took place in May 1952, even as the West and China were fighting each other at the height of the Korean War.[10] In Gardella's account, the mission entailed he and a small number of colleagues being assigned to attack a nuclear facility underneath the Sungari Reservoir near the border with North Korea (p. 99). This mission involved a team of six marines, who had purportedly received special training from the Central Intelligence Agency (CIA), prior to being parachuted into China, linking up with Nationalist Chinese sympathizers and destroying the atomic laboratory. Gardella related that his team had fought a series of battles against Communist troops during a 1,000-mile, three-week journey across northern China before being picked up in a pre-arranged rendezvous with a US submarine in the Yellow Sea. The escape saga reads like something penned by Joseph Conrad and features gun battles with the Soviets, US prisoners of war glimpsed in cages, and an escape arranged by a female fighter dubbed 'The Dragon Lady', after the character in the popular comic strip 'Terry and the Pirates'. The book was denounced as a work of fiction by the United States Marine Corps (USMC), with one unnamed officer opining that 'It is a great story that does the Corps credit, but as far as we can tell, it never happened'.[11] Such sober views were largely buried, however, as the struggle between truth and legend, once again, proved to be an unequal contest. The controversy remains undiminished and, as recently as 2010, one author evaluated the veracity of Gardella's volume in the following terms: 'Only time will tell whether this account tells of one of the [Korean] war's most bizarre covert operations or [is] a hoax.'[12]

Second, this dictionary exposes the Taiwanese intelligence agents' activities in the United States. These are seldom mentioned in other general works on Chinese intelligence. For instance, in 2004 Donald W. Keyser (the former principal deputy assistant secretary of state for East Asian and Pacific affairs), recruited by Taiwan's National Intelligence Bureau, transported numerous classified documents from the State Department to his home.[13] The documents, discovered during a search of Keyser's home on 4 September 2004, comprised some 3,559 classified pieces (including 28 deemed 'Top Secret') in hard-copy format.[14] These included ultra-sensitive documents from the Department of State, the National Security

[10] Lawrence Gardella, *Sing a Song to Jenny Next* (New York: E.P. Dutton, 1981). Gardella himself died of leukemia a few months before the publication of his book.
[11] Edwin McDowell, 'Book on Chinese Atomic Lab denied by Marine Corps', *New York Times*, 25 October 1981.
[12] Keith D. McFarland, *The Korean War: An Annotated Bibliography* (New York: Routledge, rev. 2nd edition, 2010), p. 179.
[13] J. Cole, 'Ex-US official admits taking secret papers amid Taiwanese liaison', *Agence France-Presse*, 13 December 2005.
[14] Stéphane Lefebvre, 'The Case of Donald Keyser and Taiwan's National Security Bureau', *International Journal of Intelligence and Counterintelligence*, 20/3 (2007), p. 515.

Agency, and the Central Intelligence Agency (Keyser's wife, a CIA staffer, was also discovered to have removed classified documents from the agency (p. 36)). In December 2005 Keyser pled guilty to three charges, admitting that he had removed classified documents and digital memory devices from the Department of State to his residence. He also admitted to lying the Bureau of Diplomatic Security at the Department of State about his relationship with Taiwanese intelligence. Keyser also admitted that he lied on a U.S. Customs Declaration by not listing Taiwan as a country that he had visited. In January 2007, Keyser was sentenced today to 12 months and one day in prison, fined $25,000 fine. The United States Attorney for the Eastern District of Virginia, Chuck Rosenberg, drew a line under the affair stating that Keyser 'had an absolute obligation to safeguard the classified information entrusted to him and utterly failed to do so. His sentence of imprisonment is a warning to others in positions of public trust.'[15]

One of the most intriguing entries in the dictionary concerns one Joan Hinton. Hinton, recruited to work on the wartime Manhattan Project in February 1944, collaborated with Enrico Fermi as a member of a team which 'built two reactors for testing enriched uranium and plutonium'.[16] At the ultra-secretive facility at Los Alamos, Hinton made a not inconsiderable contribution to the development of the uranium weapon ('FAT MAN') dropped on Nagasaki on 9 August (p. 111). Following the nuclear attacks on Japan, and as the Cold War intensified, a disillusioned Joan Hinton became an outspoken peace activist. In 1948, she fled to China, and then was labeled a traitor for having disclosed nuclear secrets. The furore in the US over over 'Who lost China?'[17] ('communists and queers' in the State Department according to Senator Joe McCarthy)[18] perhaps made such charges inevitable at some stage. They were rendered even more likely as China was, at that time, fighting a war against UN forces in Korea. During the McCarthy era, Hinton was accused of being an atomic spy after she addressed a peace conference in Beijing. Rear Admiral Ellis M. Zacharias (USN)[19] denounced Hinton in a 1953 article for *Real* magazine entitled 'The Atom Spy Who Got Away.' Despite such charges, there is no evidence that she ever betrayed any secrets to anyone (and, in any case, the Chinese did not attain nuclear status until 1964) or even worked as a physicist after 1948. Hinton nevertheless remained a loyal disciple of Mao Zedong to the end. In 2008, during a visit to Japan, Hinton stated that '[i]t would have been terrific if Mao had lived'. And, perhaps more

[15] Lefebvre, 'The Case of Donald Keyser and Taiwan's National Security Bureau', p. 522.
[16] V.J. Nelson, 'Joan Hinton - Oct. 20, 1921-June 8, 2010 – Joined Maoist Revolution after helping develop the atomic bomb', *Pittsburgh Post-Gazette* (PA), 24 June 2010.
[17] Stephen Glain. *State vs. Defense: The Battle to Define America's Empire* (New York: Crown, 2011), p. 68.
[18] For polemics, see John T. Flynn, *While You Slept: Our Tragedy in Asia and Who Made It* (New York: Devin-Adair, 1951); Anthony Kubek, *How the Far East Was Lost: American Policy and the Creation of Communist China, 1941-1949* (Chicago, IL: Regnery, 1963).
[19] An intelligence specialist, Zacharias (1890-1961) served in both world wars and, in the 1920s, served in Tokyo as naval attaché to the Japanese Empire. After the Second World War, he was the deputy director of US Naval Intelligence. After retiring he presented an NBC television series (*Behind Closed Doors*) which covered shadowy Cold War incidents (of which he had been involved with as a serving USN officer). The series ran for twenty-six episodes between October 1958 and April 1959.

surprisingly for a 'peace activist', she declared herself '100 percent behind everything that happened in the Cultural Revolution - it was a terrific experience.'[20] Given her life and works it is small wonder the Western intelligence community remained fascinated with Hinton's extraordinary case until long after the Cold War had ended (she died only in 2010).

Having read the *Historical Dictionary of Chinese Intelligence*, the authors clearly believed (in 2012, when the volume was published) that the US Intelligence Community (IC) regarded the People's Republic of China as *the* main global threat in the spheres of cyber-spying and cyber-espionage. Of course, recent events – not least the US presidential election of 2016 – now place Russia in that role in the opinion of most informed observers. Indeed, in early 2015, the Director of National Intelligence, James Clapper, told the Senate Armed Services Committee: 'While I can't go into detail here, the Russian cyber threat is more severe than we had previously assessed'. Clapper made this statement when presenting a report entitled *Worldwide Threat Assessment of the U.S. Intelligence Community*. This document, noting increasing Russian sophistication in this area, argued that:

> Cyber threats to U.S. national and economic security are increasing in frequency, scale, sophistication, and severity of impact … [And] Russia certainly has been more active than any other country in terms of combining cyber-attacks, or cyber-operations, with physical operations. The Russia-Georgia war of 2008 was a perfect example of a combined kinetic and cyber operation. And nobody else has ever done that – China has never done anything like that.[21]

That said, many illustrative cases of 'cyber-friction' between the PRC and the USA are included in this dictionary. These include the precautions (codenamed AVOCADO) undertaken to protect U.S. computer systems from cyber-attack (p. 23). This fits with pessimistic and unchanging forecasts, usually informed by the political ideology of Realism, made by US commentators since the end of the Cold War. As long ago as 1997 Warren I. Cohen wrote that:

> [G]enerational change will not guarantee a kinder, gentler China. Nor will the ultimate disappearance of communism in Beijing. The powerful China we have every reason to expect in the twenty-first century is likely to be as aggressive and expansionist as China has been whenever it has been the dominant power in Asia - except

[20] William Grimes, 'Joan Hinton, Physicist Who Chose China Over Atom Bomb, Is Dead at 88', *New York Times*, June11, 2010.

[21] DNI James R. Clapper, Statement for the Record to the Senate Armed Services Committee, *Worldwide Threat Assessment of the U.S. Intelligence Community*, 26 February 2015. URL:https://cdn.arstechnica.net/wp-content/uploads/2015/02/Clapper_02-26-15.pdf (accessed 5 July 2017).

> when its leaders have reason to believe that potential adversaries have both the power and the determination to stop them.[22]

It is undoubtedly the case that the PRC has sought (and seeks) to gain access to governmental, defence, financial, and technological networks within the USA. As with all modern cyber security issues, all sides are vulnerable to the smallest weaknesses in existing software. This often involves the insertion of harmful programs smuggled onto networks via the deceptively benign medium of e-mail. In 2010 the *Washington Post* reported that 'congressional and industry sources' had identified over 30 US companies (including Google, Yahoo, Symantec, Adobe, Northrop Grumman and Dow Chemical) that had been the subject of cyber-attacks emanating from China. James A. Lewis, a cyber security expert at the Center for Strategic and International Studies, stated that: 'This is a big espionage program aimed at getting high-tech information and politically sensitive information - the high-tech information to jump-start China's economy and the political information to ensure the survival of the regime'. For Lewis, this was 'what China's leadership is after. This reflects China's national priorities.'[23]

As is so often the case with powerful states, accusations of subterfuge against rising adversaries are accompanied by a real fear of the achievement of legitimate equality. In the case of the United States and the People's Republic we saw a perfect instance of the fear of competition – by both 'foul' and 'fair' means – in May 2017. This occurred when the *New York Times* reported both significant Chinese counterintelligence successes against the US[24] (which saw the killing of several CIA human 'assets'),[25] and discussed fears that the People's Republic was close to overhauling the American Republic in the crucial field of Artificial Intelligence (AI).[26]

Governments obviously neglect security measures in matters of cyber capabilities at their peril, as they were reminded when networks across the globe were attacked in May 2017. The so-called WannaCry ransomware attack targeted computers running the Microsoft Windows operating, demanding ransom payments in the Bitcoin 'cryptocurrency'. The attack affected an astonishing 230,000 computers in over 150 countries (and victims included the UK National Health Service (NHS), Spain's Telefónica, Renault of France and the German state-owned giant, Deutsche Bahn.[27]

---

[22] Cohen, 'China's Strategic Culture', p. 105.

[23] Ariana Eunjung Cha and Ellen Nakashima, 'Google China cyberattack part of vast espionage campaign, experts say', *The Washington Post*, 14 January 2010.

[24] Mark Mazzetti, Adam Goldman, Michael S. Schmidt and Matt Apuzzo, 'Killing C.I.A. Informants, China Crippled U.S. Spying Operations', *New York Times*, 20 May 2017.

[25] Eye World: 'Letter from Beijing from *Our own correspondent*', *Private Eye*, 1445, 2-15 June 2017.

[26] Paul Mozur and John Markoff, 'Is China Outsmarting America in A.I.?', *New York Times*, 27 May 2017.

[27] BBC News, 'Cyber-attack: Europol says it was unprecedented in scale', 13 May 2017. URL: http://www.bbc.co.uk/news/world-europe-39907965 (accessed 6 July 2017). Soon after the attack it was widely reported that the 'hacking tool' used against the UK National Health Service (NHS) had been developed by, and stolen from, the ultra-secretive US National Security Agency (NSA). On this,

Smith and West are virtually silent regarding the most critical challenge facing Sino-American relations in the cyber realm: namely, the phenomenon of so-called 'onion routing'.[28] Onion routing, developed by the U.S. Naval Research Laboratory in the 1990s,[29] was primarily designed to enable U.S. intelligence agents to collect information without exposing their identities or locations. Onion routing is therefore used for anonymous communication, making it much more difficult for the states to monitor intelligence activities. What does the onion routing mean to Chinese intelligence in the foreseeable future? Alas, the dictionary has little to say on the matter. Omissions on onion routing notwithstanding, the *Historical Dictionary of Chinese Intelligenc*e represents a decent survey of the dynamics of Chinese intelligence and counter-intelligence, past and present. This dictionary should be required reading for all those who are interested in such matters, as well as anyone who wishes to engage in scholarly debates on the evolution of. Comprising a veritable cornucopia of information, the *Historical Dictionary of Chinese Intelligenc*e deserves a place in the Intelligence Studies literature and would a useful addition to the library of anyone interested in Sino-American relations, Chinese politics and the history of Chinese foreign policy.

R. Gerald Hughes
Aberystwyth University
Email: rbh@aber.ac.uk

Kai Chen
Xiamen University
Email: kaichen@xmu.edu.cn

References

- BBC News, 'Cyber-attack: Europol says it was unprecedented in scale', 13 May 2017. URL: http://www.bbc.co.uk/news/world-europe-39907965 (accessed 6 July 2017).
- Henry Bodkin, Barney Henderson, Laura Donnelly, Robert Mendick, Ben Farmer and Chris Graham, 'Government under pressure after NHS crippled in

see Henry Bodkin, Barney Henderson, Laura Donnelly, Robert Mendick, Ben Farmer and Chris Graham, 'Government under pressure after NHS crippled in global cyber attack as weekend of chaos looms', *Daily Telegraph*, 13 May 2017. The intense speculation about the NSA's role in the 2017 attacks typifies the manner in which, in all matters pertaining to intelligence and/or espionage, the media immediately embrace gossip and rumour-mongering as much as they ever did.

[28] In short, 'Onion routing' consists of a technique for sending anonymous communications over a computer network. 'Onion routing is intended to provide real-time bidirectional anonymous connections that are resistant to both eavesdropping and traffic analysis in a way that is transparent to applications.' Marco Cremonini, Chiara Braghin and Claudio Agostino Ardagna, 'Privacy on the Internet' in John R. Vacca (ed.), *Computer and Information Security Handbook* (Boston, MA: Morgan Kaufmann, 2nd edition, 2013), p. 748.

[29] P. Tucker, 'The Online Habits That Trigger NSA Spying', *National Journal*: Web Edition Articles (USA), 8 December 2015.

global cyber attack as weekend of chaos looms', *Daily Telegraph*, 13 May 2017.
- Ariana Eunjung Cha and Ellen Nakashima, 'Google China cyberattack part of vast espionage campaign, experts say', *The Washington Post*, 14 January 2010.
- David Ian Chambers, 'Edging in from the Cold: The Past and Present State of Chinese Intelligence Historiography', *Studies in Intelligence*, 56/3 (2012), pp. 31-46.
- DNI James R. Clapper, Statement for the Record to the Senate Armed Services Committee, *Worldwide Threat Assessment of the U.S. Intelligence Community*, 26 February 2015. URL:https://cdn.arstechnica.net/wp-content/uploads/2015/02/Clapper_02-26-15.pdf (accessed 5 July 2017).
- Warren I. Cohen, 'China's Strategic Culture', *Atlantic Monthly*, 279/3 (1997), pp. 103-5.
- J. Cole, 'Ex-US official admits taking secret papers amid Taiwanese liaison', *Agence France-Presse*, 13 December 2005.
- Marco Cremonini, Chiara Braghin and Claudio Agostino Ardagna, 'Privacy on the Internet' in John R. Vacca (ed.), *Computer and Information Security Handbook* (Boston, MA: Morgan Kaufmann, 2nd edition, 2013).
- Eye World: 'Letter from Beijing from *Our own correspondent*', *Private Eye*, 1445, 2-15 June 2017
- John T. Flynn, *While You Slept: Our Tragedy in Asia and Who Made It* (New York: Devin-Adair, 1951).
- Lawrence Gardella, *Sing a Song to Jenny Next* (New York: E.P. Dutton, 1981).
- Stephen Glain. *State vs. Defense: The Battle to Define America's Empire* (New York: Crown, 2011).
- William Grimes, 'Joan Hinton, Physicist Who Chose China Over Atom Bomb, Is Dead at 88', *New York Times*, 11 June 2010.
- Anthony Kubek, *How the Far East Was Lost: American Policy and the Creation of Communist China, 1941-1949* (Chicago, IL: Regnery, 1963).
- Stéphane Lefebvre, 'The Case of Donald Keyser and Taiwan's National Security Bureau', *International Journal of Intelligence and Counterintelligence*, 20/3 (2007), pp. 512-26.
- Peter Mattis, review of I.C. Smith and Nigel West, *Historical Dictionary of Chinese Intelligence* in *Studies in Intelligence*, 56/4 (2012), pp. 21-3.
- Peter Mattis, 'Five Ways China Spies', *The National Interest*, 6 March 2014.
- Mark Mazzetti, Adam Goldman, Michael S. Schmidt and Matt Apuzzo, 'Killing C.I.A. Informants, China Crippled U.S. Spying Operations', *New York Times*, 20 May 2017.
- Paul Mozur and John Markoff, 'Is China Outsmarting America in A.I.?', *New York Times*, 27 May 2017.
- Edwin McDowell, 'Book on Chinese Atomic Lab denied by Marine Corps', *New York Times*, 25 October 1981.
- Keith D. McFarland, *The Korean War: An Annotated Bibliography* (New York: Routledge, rev. 2nd edition, 2010).

- V.J. Nelson, 'Joan Hinton - Oct. 20, 1921-June 8, 2010 – Joined Maoist Revolution after helping develop the atomic bomb', *Pittsburgh Post-Gazette* (PA), 24 June 2010.
- Sergey Radchenko, review of Michael Schoenhals, *Spying for the people: Mao's secret agents, 1949–1967*, *Intelligence and National Security*, 31/6 (2016), pp. 928-9.
- Michael Schoenhals, *Spying for the people: Mao's secret agents, 1949–1967* (Cambridge: Cambridge University Press, 2013).
- Sun Tzu, *The Art of War* (Oxford: Oxford University Press, 1963).
- P. Tucker, 'The Online Habits That Trigger NSA Spying', *National Journal*: Web Edition Articles (USA), 8 December 2015
- Xuezhi Guo, *China's Security State: Philosophy, Evolution and Politics* (Cambridge: Cambridge University Press, 2012).