Final conclusions

The introduction began by outlining China's rise as a major world power, its political and economic system, and how it has theorized the uses of cyber and technology to enhance its economy, military, and political influence. It showed how China is an expanding power ruled since 1949 by the Communist Party of China (CCP) and whilst there are concerns of Westernization and "splittism" or state fragmentation from within, the binding of party–state remains intact. At the same time the CCP and People's Liberation Army (PLA) have theorized and operationalized forms of political warfare amplified by Information Communications Technologies (ICT).[1]

China's Belt and Road Initiative (BRI) is a modern-day Silk Route for both overland and maritime trade. What is more, the CCP has an eye to the militarization of these routes, especially in naval bases stretching from the Indian Ocean to the Horn of Africa. Across land, sea, air, and space, China has made rapid advances. Where once its military was dominated by its massive number of ground forces, designed to fight a defensive war from within China, it now boasts capabilities and numbers at sea, in the air, and orbiting around the earth that enable a host of possibilities. The fifth domain of warfare, cyber, has been a major enabler through cyberespionage.

China closely examined Western developments to close the gap on the West and rest of the world, simultaneously allowing it to grow its regional ambitions and those of the BRI. In the politico-military realm the PLA took on board a number of lessons, beginning with the 1991 Gulf War. The PLA oversees "the full space enterprise", including military and civilian integration, and shadowed the U.S. approach.[2] They looked at how command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR), enabled by satellites for intelligence sharing, were used to fully utilize the asymmetric military advantage held by U.S.-led coalition forces. The value of this was further confirmed during the Second Gulf War in 2003.

The uses and usefulness of this approach were viewed as a force multiplier to air, land, and maritime forces, aided by space and America's network of satellites. U.S. ideas of Network-Centric Warfare and replicating and enhancing a system-of-systems approach came to inform PLA thinking. This led one Chinese General to comment, "Our sights must not be fixed on the firepower warfare of the industrial

1 Dean Cheng, *Cyber Dragon: Inside China's Information Warfare and Cyber Operations* (Santa Barbara, CA: Praeger, 2017), pp. 41–48.

2 Caitlin Campbell, "China's Military: The People's Liberation Army (PLA)" (June 4 2021), p. 43, accessed November 8 2021.

https://doi.org/10.1515/9783111575513-008

age, rather they must be trained on the information warfare of the information age".[3] PLA theory and stratagems, built on the military philosophy of Sun Tzu and to a lesser extent Mao Zedong's "People's War", borrowed from Western concepts but through some innovative thinkers the PLA also began to transform its armed forces and grow its economy. It is also impressive evidence that the demise of the USSR and Soviet-inspired communism was not, as Francis Fukuyama contended, *The End of History.*[4]

Under President Xi Jingpin China has continued to make significant advances, and like his immediate predecessors Jiang Zemin (1989–2002) and Hu Jintao (2002–2012), Xi has overseen military modernization and made it a high priority. This has seen PLA ground forces advance, with the PLA now supplied with a diverse array of modern military equipment complementing a slimmed-down force (post-2015) of around one million *army* ground forces. Periodic restructures of the PLA have been one of the features of Xi's time in office. It was stated in the introduction that under Xi the CCP set about achieving three forward-thinking aims for the PLA. These were to achieve mechanization of the PLA by 2020, alongside networking its assets to improve efficiency and promote jointness; to complete this modernization process by 2035; and achieve a world-class military by 2049, the hundredth anniversary of the founding of the People's Republic of China (PRC).[5] These plans are on track.

This includes its tanks, helicopters, and amphibious forces. The PLA Air Force (PLAAF) continues to replace older aircraft with fourth-generation or higher. Its suite of missiles, overseen by the PLA Rocket Force (PLARF), has similarly developed and diversified. By 2015–2017, China was considerably ahead of the United States Navy (USN) in shipbuilding (measured by tonnage). Although combat effectiveness remains to be seen, since 2020 the PLA Navy has become the world's largest navy in terms of raw numbers (with massive expansion both quantitatively and qualitatively).[6] It is rapidly becoming a Mahanian "blue water" navy capable of power projection. Two older-generation aircraft carriers are already deployed, a

3 Major General Wang Pufeng, "The Challenge of Information Warfare", *China Military Science* (1995), https://fas.org/irp/world/china/docs/iw_mg_wang.htm, accessed March 28 2019.

4 Francis Fukuyama, "The End of History", *National Interest*, No. 16 (Summer 1989), pp. 3–18. Francis Fukuyama, *The End of History and the Last Man* (New York: Free Press, 1992). Francis Fukuyama, "The 'End of History' 20 Years Later", *New Perspectives Quarterly*, Vol. 27, Issue 1 (Winter 2010), pp. 7–10.

5 Campbell, "China's Military: The People's Liberation Army", Summary.

6 Nick Childs and John Waldwyn, "China's Naval Shipbuilding: Delivering on Its Ambition in A Big Way" (May 1 2018), https://www.iiss.org/blogs/military-balance/2018/05/china-naval-shipbuilding, accessed April 13 2018.

third is being built, with four more currently envisaged. These later carriers will likely have the latest electromagnetic catapults and the most modern suite of technologies and weapons in China's inventory.

Whilst its ground forces have decreased, in total across all its service branches, the PLA calls on around two million active service personnel.[7] Its military budget is second only to that of the United States.[8] Through cyberespionage from the West, especially companies in the United States, it has also achieved a bigger bang for the buck by surreptitiously gaining access to American research and development (R&D), greatly reducing its spend and circumventing challenging military developments and the need to innovate for itself. It has done the same across civilian industries from wind turbines to robotics, and from manufacturing through to medicine, with a policy to introduce, digest, assimilate, and re-innovate within China.

1 PLA structure, restructuring, and Chinese intelligence

Relatedly, the introduction also characterized the domestic structure of China's government and the PLA. The structure of the General Staff and the major General Staff Departments of 2PLA, 3PLA, and 4PLA were then outlined. It described that 2PLA was responsible for Human Intelligence collection and analysis (HUMINT); 3PLA Signals Intelligence; and 4PLA Electronic Intelligence and offensive "electronic warfare". Organizationally, this has traditionally been supported by at least 28 technical reconnaissance bureaus.

2PLA also contained Unit 61398, which is alleged to be home to some of the most virulent Advanced Persistent Threat (APT) groups in the world. These have been accused of a wide variety of cyberespionage campaigns across the defense industrial base, concentrated on the United States. 3PLA has often been equated to the U.S. National Security Agency (NSA), with facilities in several Chinese cities and a presence in all seven (pre-2024) military regions. 4PLA was believed to have responsibility for executing China's cyberwarfare stratagems, including against critical infrastructure (CI).

The PLA, much like China itself, has however been on a process of reforms and reorganization, and between late 2015 and early 2016 "Xi announced the

7 Campbell, "China's Military: The People's Liberation Army", pp. 8, 34–39, 52–53. Roy D. Kamphausen (ed.), *The People of the PLA 2.0* (Carlisle, PA: US Army War College Press, 2021).

8 Nan Tian and Fei Su, "A New Estimate of China's Military Expenditure" (January 2021), https://www.sipri.org/sites/default/files/2021-01/2101_sipri_report_a_new_estimate_of_chinas_military_expenditure.pdf, accessed November 8 2021.

most ambitious reform and reorganization of the PLA since the 1950s".[9] These reforms included increasing joint operations and a reshaping of internal cyber operations. This encompassed PLA ground forces, the PLAN, PLAAF, PLARF, and established the PLA Joint Logistics Support Force (in 2016). It also notably led to the formation in 2015 of the PLA Strategic Support Force (PLASSF). This centralized information and space operations. This included cyber, electronic, and psychological warfare.[10]

This was a step towards improving jointness between the component branches of the PLA. In 2024 another phase of military reorganizations was announced. This saw the reorganization or disbandment of the PLASSF into separate but interrelated organizations. These are the Military Aerospace Force, Cyberspace Force, and Information Support Force. All operate under the Central Military Commission (CMC), China's equivalent to the Pentagon. As well as being a third-term president, Xi is also General Secretary of the CCP and Chairman of the CMC.[11] This centralization of power and accusations of authoritarianism have arrived with anti-corruption drives (and the unexplained removal of officials) and the public ejection of former premier Hu Jintao from the 20th Party Congress in 2022, whilst increasingly binding the party–state system through party-centric nationalism.[12]

The 2024 reforms might be the culmination of a process of mini reorganizations between 2017 and 2024.[13] This saw the Central Cybersecurity and Informatization Leading Group, established in 2013, become the Central Cyberspace Affairs Commission in 2018. It also saw the Cyberspace Administration of China and the Ministry of Industry and Information Technology play important coordinating

9 Campbell, "China's Military: The People's Liberation Army", p. 10.

10 Campbell, "China's Military: The People's Liberation Army", p. 40.

11 "Xi Jinping 习近平", https://www.brookings.edu/wp-content/uploads/2018/03/china_20180318_xi_jinping_profile.pdf, accessed February 24 2024.

12 Steve Tsang and Olivia Cheung, "Has Xi Jinping Made China's Political System More Resilient and Enduring?", *Third World Quarterly*, Vol. 43, Issue 1 (2022), pp. 225–243. Horst Fabian and Andreas Fulda, "The End of the China Illusion" (November 7 2022), https://www.rusi.org/explore-our-research/publications/commentary/end-china-illusion, accessed November 8 2024.

13 Joe McReynolds and John Costello, "Planned Obsolescence: The Strategic Support Force In Memoriam (2015–2024)", https://jamestown.org/program/planned-obsolescence-the-strategic-support-force-in-memoriam-2015-2024/ and J. Michael Dahm, "A Disturbance in the Force: The Reorganization of People's Liberation Army Command and Elimination of China's Strategic Support Force", *China Brief*, Vol. 24, Issue 9 (April 26 2024), https://jamestown.org/program/a-disturbance-in-the-force-the-reorganization-of-peoples-liberation-army-command-and-elimination-of-chinas-strategic-support-force/. Both accessed September 1 2024.

roles alongside the Ministry of Science and Technology. This, and more, was outlined and discussed in chapter 1.[14]

With improving jointness a clear priority, the PLA and CCP have paid close attention to Russia's military performance in the Ukraine War. Russia has attempted jointness across the five domains of warfare (land, sea, air, space, and cyberspace). It has not been successful. The Russian military is a different beast, but coordinating across the five domains (including combined arms operations akin to World War II) has led to a "meat grinder" on the front lines. Not only have Russia's primary aims proved wishful thinking, but attacking forces have also been continually blunted.[15] For the PLA, as "a ship being rebuilt while also underway", jointness can expose "hidden weaknesses and fundamental faults".[16] This can only be fully tested in battle.

Reforms have also seen the Ministry of State Security (MSS) conduct campaigns alongside units from the PLA. The MSS, previously responsible for civilian intelligence and counterintelligence, now stands accused of both cyberespionage and cybercrimes against companies in the commercial sector alongside the PLA.[17] The introduction also outlined that alongside cyberespionage, China, as well as many other nations, continues to use traditional espionage as standalone intelligence-gathering activities and as an aid to cyberespionage.

This includes the recruitment of (and attempts to recruit) foreign government agents and politicians, as well as targeting company employees in the private sector. This involves allegations of bribery, blackmail, the use of honey traps and "swallows" ("sexploitation"), and "spotters" who will identify potential targets and then pass them to an intelligence officer for further assessment.[18] This embrace of HUMINT includes utilizing Chinese officials with diplomatic cover and

---

14 Tai Ming Cheung, "The Rise of China as a Cybersecurity Industrial Power: Balancing National Security, Geopolitical, and Development Priorities", *Journal of Cyber Policy*, Vol. 3, No. 3 (2018), pp. 316–318. Jamie P. Horsley, "Behind the Facade of China's Cyber Super-regulator: What We Think We Know – and What We Don't – about the Cyberspace Administration of China" (August 8 2022), https://digichina.stanford.edu/work/behind-the-facade-of-chinas-cyber-super-regulator/, accessed August 21 2024.

15 Kristan Stoddart, "Russia's Cyber Campaigns and the Ukraine War: From the 'Gray Zone' to the 'Red Zone'", *Applied Cybersecurity & Internet Governance*, Vol. 3, No. 1 (June 2024), pp. 5–33.

16 David Chen, "Lessons of Ukraine Raise Doubts about PLA Modernization" (April 8 2022), https://jamestown.org/program/lessons-of-ukraine-raise-doubts-about-pla-modernization/, accessed October 25 2024.

17 "Most Wanted", https://www.fbi.gov/investigate/cyber/most-wanted, accessed November 3 2024.

18 Hollie McKay, "China's Extensive 'Honey Trap' Spy Network could Involve Thousands of Ploys Underway Now, Ex-operative Says" (December 10 2020), https://www.foxnews.com/politics/how-china-has-built-its-extensive-honey-trap-spy-network, accessed November 27 2021.

diplomatic immunity and those operating under "Non-Official Cover" or "Illegals", who act covertly (and lack diplomatic immunity).[19]

As well as "the recruitment of foreign nationals to conduct espionage", HUMINT embraces "the use of travelers to gather intelligence, as well as the debriefing of defectors and other individuals with access to information of value".[20] HUMINT requires a great deal of time and resources in creating assets, running them, and analyzing the intelligence-information they produce (which for states like China means integrating this into the intelligence cycle). It can be high risk, financially expensive, and require a great deal of complex effort and judgment to work in potentially hostile environments. This means field agents are required to learn foreign languages, detection techniques, surveillance and surveillance avoidance, recruitment skills, self-defense skills, and so on.

In a world of CCTV, cell phones with high-resolution cameras and high-quality audio and video recording, and biometrics including facial recognition, surveillance and counterintelligence are made easier. Conversely, surveillance avoidance is made more difficult. Moreover, open-source intelligence (OSINT) (including social media intelligence) can exploit the digital footprints left by people and companies, to target and gather intelligence. This can also be used for counterintelligence against those trying to hide in the shadows or using false identities. Additionally, consumer devices like smartphones, micro-sized SD cards, and USB sticks make it easier to implant code and have even greater uses in exfiltrating information and intelligence against hard targets that are too difficult to hack remotely.

Agents (spies) and insiders can be used to infect devices and computer systems as well as gathering intelligence.[21] Although China prioritizes, and has greatly exploited, remote access (cyberespionage), the technologies and tradecraft described above are also an option, especially against foreign travelers within China. China is also alleged to use its expatriate community including Chinese businesspeople, companies, and academics at home and abroad, including through the "Thousand Talents Program". It has also invested in or purchased companies working on tech-

19 Jury Convicts Chinese Intelligence Officer of Espionage Crimes, Attempting to Steal Trade Secrets (November 5 2021), https://www.justice.gov/opa/pr/jury-convicts-chinese-intelligence-officer-espionage-crimes-attempting-steal-trade-secrets. Garrett M. Graff, "China's 5 Steps for Recruiting Spies" (October 31 2018), https://www.wired.com/story/china-spy-recruitment-us/. Both accessed November 21 2021.

20 Jeffrey T. Richelson, "The Pentagon's Spies" (July 6 2015), https://nsarchive2.gwu.edu/NSAEBB/NSAEBB520-the-Pentagons-Spies/, accessed January 27 2020.

21 Joel Brenner, *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare* (New York: Penguin Press, 2011), pp. 82–90.

nologies or products in sectors of strategic benefit to China. These have all been key enablers of China's rapid development and its rising power.[22]

One view of China's rise and its view of the international system were set out in January 2013 by Lieutenant General Qi Jianguo, then recently appointed as Deputy Chief of the General Staff with responsibility for foreign relations and intelligence. He wrote in the official weekly newspaper of the CCP's Central Party School:

> In the next decade or two, it is possible that the initial framework of a multipolar world will take shape. However, a power's rise and decline is a complex and lengthy process and it will be a long process of development before a global multipolar framework emerges … The end of the Cold War marked the first time in the 500 year rise of the West that a transformation of the international framework was completed without conflict. Twenty years later, mutual cooperation and competition between great powers exists and overlapping interests are interwoven with the strategic game [*zhanlue boyi*; 战略博 弈]; the risk of all-out confrontation has declined, and great power relations have entered a new phase of development. Great power interests are deeply blended … with the deepening development of economic globalization, the interests of each country are blending together as are crises. A problem in any one country may affect other nations … in particular, there must be strategic foresight [*zhanlue yuanjian*; 战略远见] for the development of Sino-U.S. relations … Cybersecurity [*wangluo anquan*; 网络安全] concerns national sovereignty as well as the security of economic and social operations, and it concerns the quality of human existence. The West's so-called "internet freedom" actually is a type of cyber-hegemony [*wangluo ziyou*; 网络自由]. In the information era, seizing and maintaining superiority in cyberspace is more important [*gengwei zhongyao*; 更为重要] than seizing command of the sea and command of the air were in World War II.[23]

This summarizes some of China's thought processes but what Qi omitted was that China's embrace of cyber, especially cyberespionage, has enabled the PLA's growing ability to challenge at sea, in the air, on land, and in space, as well as cyberspace. These thought processes were examined in chapter 1, which analyzed Chinese theories and theoreticians on cyber as an evolution from 1991 through to the present to increase our understanding of Chinese cyberespionage campaigns and targets, as well as thinking on cyberwarfare.

---

22 Whether this is all part of a grand plan to reorder the world is the subject of Clive Hamilton and Mareike Ohlberg, *Hidden Hand: Exposing How the Chinese Communist Party is Reshaping the World* (London: Oneworld Publications, 2020).

23 Qi Jianguo, "An Unprecedented Great Changing Situation: Understanding and Thoughts on the Global Strategic Situation and Our Country's National Security Environment", in-house translation by James A. Bellacqua and Daniel M. Hartnett, CNA China Studies Division, https://www.cna.org/CNA_files/PDF/DQR-2013-U-004445-Final.pdf, accessed April 9 2019.

2 From unrestricted warfare to seizing information supremacy

The release in 1999 of *Unrestricted Warfare*, a treatise widely read in China's political and military circles, written by two Chinese colonels (Qiao Liang and Wang Xiangsui) began a process of innovation in Chinese thinking. They believed a Revolution in Military Affairs had taken place. In their eyes the battlefield was everywhere. Conventional military force in the pursuit of political ends was but one arrow in the quiver. They suggested that American and Western technological advantages had also made them reliant on technology and this could be exploited. Through technology, economies could be manipulated, computer viruses implanted, and social and psychological warfare conducted.[24]

It was years before similar ideas arrived in the West.[25] Qiao and Wang were writing at the dawn of the modern Internet, before social media, and predating the massive increase in always-on connectivity. Although economic espionage, psychological operations, propaganda, disinformation campaigns, and double cross have long existed (including in World War II), there was much that was new. Sharing similarities with Russia's later embrace of "hybrid warfare", Qiao and Wang wrote that Unrestricted Warfare embraces everything from military hard power to socio-economic–cultural soft power "to compel the enemy to accept one's interests" whilst falling in the "gray zone" between peace and conflict.[26]

Unrestricted Warfare sparked a debate which led into discussions of "Acupuncture/Paralysis Warfare" which looked to hit the weak links in command, control, communications, and intelligence chains. By 2000, Information Warfare departments had been established by the PLA and another colonel, Shen Weiguang, had conceived the concept of Total Information War, which borrowed from and fleshed out some of the ideas that evolved after *Unrestricted Warfare*, including "acupuncture/paralysis warfare".[27]

---

24 Qiao Liang and Wang Xiangsui, *Unrestricted Warfare: China's Master Plan to Destroy America* (Brattleboro, VT: Echo Point, 2017), pp. 43, 120, in Timothy L. Thomas, *The Dragon's Quantum Leap: Transforming from a Mechanized to an Informatized Force* (Fort Leavenworth, KS: Foreign Military Studies Office, 2009), pp. 29–30.

25 Frank G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars* (Arlington, VA: Potomac Institute for Policy Studies, 2007).

26 Qiao and Wang, *Unrestricted Warfare*, pp. xxi-xxii.

27 Shen Weiguang, *Deciphering Information Security* (Beijing: Xinhua Publishing House, 2003), pp. 380–405. Quoted in Timothy L. Thomas, *Decoding the Virtual Dragon: Critical Evolutions in the Science and Philosophy of China's Information Operations and Military Strategy* (Fort Leavenworth, KS: Foreign Military Studies Office, 2007), p. 134 and Thomas, *The Dragon's Quantum Leap*, pp. 146–147.

These developments were closely followed by the 2001 Science of Military Strategy (SMS). This laid out five areas to develop: Intelligence Warfare; Command and Control Warfare; Electronic Warfare; Cyberwarfare; and Destructive Warfare. These were looked at with a view to gaining information superiority, aimed at "attacking, weakening, and interfering with enemy information systems", but with defensive and protective provisos (a recognition of China's own vulnerabilities).[28] The 2001 SMS also made the first mention of Strategic Psychological War (SPW) to undermine civilian populations and military morale and as a method of countering Western propaganda. SPW built on a key principle of Sun Tzu – to subdue an enemy without fighting.[29]

These ideas were developed further by Major General Dai Qingmin in his 2008 book *New Perspectives on War*.[30] Dai had become known for his work "On Seizing Information Supremacy" which appeared in 2002. His thoughts on these and other related issues were also influential in the PLA and CCP. In peace and war, Dai felt China's technological disadvantages could be alleviated by gaining "information supremacy" through the infiltration of Western networks and systems, and knowledge of Western military systems and networks, as well as peacetime covert attacks against CI.[31] This influenced the CCP's concept of the "Three Warfares" (psychological, legal, and public opinion warfare) enabled through integrated network and Electronic Warfare. This was refined as "winning without fighting", another Sun Tzu maxim, where space was seen as a commanding height which included potential offensive use of anti-satellite weapons.[32]

There were also advocates for computer network attacks against the CI of rival states dating from the 2001 SMS. This included civilian targets such as ports and

28 Timothy L. Thomas, *Dragon Bytes: Chinese Information-War Theory and Practice* (Fort Leavenworth, KS: Foreign Military Studies Office, 2004), p. 39. For an overview of some of these vulnerabilities see P.K. Mallick, *China in the Cyber Domain* (New Delhi: Vivekananda International Foundation/Prints Publications, 2022), pp. 348–364.

29 Peng Guangqian and Yao Youzhi, *The Science of Military Strategy*, English translation (Shanghai: Military Science Publishing House, 2005), pp. 146–147, 202–206, 362–376. In Thomas, *Decoding the Virtual Dragon*, pp. 24, 27–29.

30 Dai Qingmin, *New Perspectives on War* (Beijing: PLA Publishing House, 2008). The title can also be translated as *War in New Perspective.*

31 Dai Qingmin, *Wangdian Yiti zhan Yinlun* (*Introduction to Integrated Network and Electronic Warfare*) (Beijing: PLA Press, 2002), pp. 79, 110, 151, 170, 194, 266, 284–287. Quoted in Thomas, *Decoding the Virtual Dragon*, pp. 104–105.

32 Dean Cheng, "Winning Without Fighting: The Chinese Psychological Warfare Challenge" (July 12 2013), https://www.heritage.org/global-politics/report/winning-without-fighting-the-chinese-psychological-warfare-challenge, accessed March 4 2020.

airports.[33] Suggestions also began to be made to embed malware in foreign weapons systems as "kill-switches" that could stay dormant until activated. Plans had also been discussed to leverage sub-state Chinese hackers for foreign operations. In 2009, the head of cybersecurity research at the PLA's famed Academy of Military Science suggested attacking CI for disruption or damage. This included power systems, telecommunications, and education.[34]

By this point, although cyber deterrence had been considered, it was seen through the lens and lessons learned in the nuclear weapons domain (as it was in the West).[35] Cyber has different characteristics and this makes directly or indirectly cross-applying nuclear deterrence theories and concepts problematic. This includes concepts such as pre-emption/first strike, retaliation, survivability, and escalation control.[36]

After the 2013 SMS, new stratagems for Information Warfare were being encouraged to complement the military reforms then underway (culminating in 2015). This included improved situational awareness, cyber defenses, and exploration of international cyber cooperation. This is what led to the PLASSF, and the Obama–Xi agreement, alongside heightened national network and information security and domestic measures aimed at monitoring social stability.[37]

After 2015, developments in the field of Artificial Intelligence (AI) became the subjects of increasing discussion. This was considered not only as part of the offense but also as an aid to jointness.[38] There was also a move away from informatized to intelligentized warfare. This, too, was seen as a means to help overcome difficulties with mounting, sustaining, and optimizing jointness across domains

---

33 Min Zengfu, *Kongjun Junshi Sixiang Gailun* (*An Introduction to PLA Air Force Military Thought*) (Beijing: Military Science Press, 2006), pp. 175–176. See also Jiang Yamin, *Yuan Zhan* (*Long Distance Operations*) (Beijing: Military Science Press, 2007), pp. 133–140. Both in Larry M. Wortzel, *The Chinese People's Liberation Army and Information Warfare* (Carlisle, PA: United States Army War College Press, 2014), p. 56.

34 Zhang Ying, "Zhanlue Pouxi: Zhonguo Bixu An Junshi Duikang Yuanze Yanjiu Wangge Zhan" ("Strategic Analysis: China Must Research Cyber Warfare According to the Principles of Military Confrontation"), *Dongfang Zaobao* (*Oriental Morning Post*), July 9 2009. Both in Wortzel, *The Chinese People's Liberation Army and Information Warfare*, p. 54.

35 Thomas, *Dragon Bytes*, pp. 35–36.

36 Kristan Stoddart, *Cyberwarfare: Threats to Critical Infrastructure* (London: Palgrave/Springer, 2022), pp. 1–51, 401–429 (introduction and conclusion).

37 "Full text: China's Military Strategy (Xinhua)" (May 26 2015), http://www.chinadaily.com.cn/china/2015-05/26/content_20820628_2.htm, accessed February 1 2019.

38 Timothy Thomas, *The Chinese Way of War: How Has it Changed?* (McLean, VA: Mitre Corporation/US Army Futures and Concepts Center, 2020), pp. 2–3, https://community.apan.org/cfs-file/__key/docpreview-s/00-00-16-68-30/20200611-China-Way-of-War-_2800_Timothy-Thomas_2900_.pdf, accessed August 24 2024.

and environments.[39] Much of this (then and now), is driven by ideas of *Shi*, which at its base is looking for advantage or superiority.[40]

There was also renewed interest in the electromagnetic spectrum for defensive and offensive action.[41] This included 2018/19 discussions of improving the use of Electronic Intelligence for intelligence, surveillance, and reconnaissance to better enable operations from commanding heights through to field-level decisions. This would also help cross-domain integration. This was also set in the context of the critical nodes of CI and Psychological Operations, including the use of propaganda (incorporating mis- and disinformation), and the utilization of deception. This harked back to ideas found in *Unrestricted Warfare* and later theoreticians like Shen, and theorems including SPW and the "Three Warfares".[42]

AI was conceived of as a key tool enabling deception through fake messages and messengers whilst aiding battlespace decisionmaking.[43] Some believed it could demist the "fog of war".[44] Morality and ethics (two fundamental components of International Humanitarian Law and the Law of Armed Conflict) were also regularly discussed in the late 2010s. This included concerns about AI, Machine Learning, machine-on-machine warfare, and cognitive warfare.[45]

---

39 Ben Noon and Chris Bassler, "Schrodinger's Military? Challenges for China's Military Modernization Ambitions" (October 14 2021), https://warontherocks.com/2021/10/schrodingers-military-challenges-for-the-chinas-military-modernization-ambitions/, accessed October 23 2021.

40 Thomas, *The Chinese Way of War: How Has it Changed?*, pp. 3–4, 21–22, 24–26.

41 Shan Linfeng, Jin Jiacai, and Zhang Ke, *Dianzi Duikang Zhisheng Jili* [电子对抗制胜机理] (*The Winning Mechanism of Electronic Countermeasures*) (Beijing: National Defense Industry Press, 2018), pp. 13–15, 26, 39–40, 48.

42 Linfeng et al., *The Winning Mechanism*, pp. 39–41, 46–48, 55, 63, 67, 74, 83–87, 92–94, 103, 106, 117–118, 141, 146–149, 158–159, 163–164, 172, 180–181. See also Zi Yang, "PLA Stratagems for Establishing Wartime Electromagnetic Dominance: An Analysis of 'The Winning Mechanisms of Electronic Countermeasures'", *China Brief*, Vol. 19, Issue 3 (February 1 2019), https://jamestown.org/program/pla-stratagems-for-establishing-wartime-electromagnetic-dominance-an-analysis-of-the-winning-mechanisms-of-electronic-countermeasures/, accessed August 30 2024.

43 Wang Yonghua, "A Study of the Key Points for Winning Intelligentized Warfare", *Jiefangjun Bao Online*, March 29 2018. Quoted in Thomas, *The Chinese Way of War: How Has it Changed?*, p. 30.

44 Li Minghai, "Where Exists the War-Winning Mechanisms of AI Warfare", *Jiefangjun Bao*, January 15 2019. Quoted in Thomas, *The Chinese Way of War: How Has it Changed?*, p. 34.

45 Wang Chunfu, "Bring Military AI Implementation onto the Track of Scientific Development", *Jiefangjun Bao Online*, March 26 2019. Gu Jingchao and Liu Kui, "Be Discreet about 'Autonomous Decision-Making' in AI-Based Military Command", *Jiefangjun Bao Online*, March 26 2019. Yuan Yi, Gao Dongming, and Zhang Yujun, "Autonomous Decision-Making in Intelligent Command", *Jiefangjun Bao Online*, April 18 2019. Yang Wenzhe, "How to Win Intelligentized Warfare by Analyzing What Has Changed and What Has Not Changed", *Jiefangjun Bao*, October 22 2019. Xu Weiwei and Li Huan, "The Main Types of Drone Swarm Warfare", *Jiefangjun Bao*, January 23 2020. All referenced in Thomas, *The Chinese Way of War: How Has it Changed?*, pp. 35–37.

During the Covid-19 pandemic (2019–2022), more thought was given over to foreign and domestic propaganda and "thought management" (思想管理).[46] AI was part of that conversation, as were its continuing offensive and defensive uses.[47] This was part of the search for the intelligentized high ground.[48] Discussion has also been given over to deterrence by denial and Cyber Mimic Defense.[49] Theorists who advocated launching pre-emptive attacks and possible large-scale cyberwarfare have diminished, but whether ideas promoting international norms gain meaningful traction remains to be seen.[50] This reflects the two strands of Chinese strategic culture outlined in the introduction and in evidence at points throughout: the neorealist "parabellum" that is prepared to use force to achieve objectives, and the defensive, non-aggressive, morally guided "Confucian-Mencian" strands. Strategic culture also resonates at the service level and the values and missions of the PLA and China's intelligence services.[51]

Lastly, chapter 1 outlined how Sino-Russian dialogues and military-to-military technology transfers have also aided development and augmented China's growing strength and assertiveness. This was enhanced in 2015 through a Sino-Russian non-aggression cybersecurity agreement whose provisions go beyond non-aggression into cooperation. They have also announced plans for increasing cooperation in space ventures (including on the moon).[52] Given a Cold War history of competition

46 Devin Thorne, "AI-Powered Propaganda and the CCP's Plans for Next-Generation 'Thought Management'", *China Brief*, Vol. 20, Issue 9 (May 15 2020), https://jamestown.org/program/ai-powered-propaganda-and-the-ccps-plans-for-next-generation-thought-management/, accessed August 31 2024.

47 John Chen, "Cyber and Influence Operations", in William C. Hannas and Huey-Meei Chang (eds.), *Chinese Power and Artificial Intelligence* (Abingdon: Routledge, 2023), pp. 189–205.

48 Elsa B. Kania, "The PLA Strategic Support Force: Innovating for Future Warfare", in James Char (ed.), *Modernising the People's Liberation Army: Aspiring to be a Global Military Power* (Abingdon: Routledge, 2024), pp. 160–185.

49 See for example Zequan Chen, Gang Cui, Lin Zhang, Xin Yang, Hui Li, Yan Zhao, Chengtao Ma, and Tao Sun, "Optimal Strategy for Cyberspace Mimic Defense Based on Game Theory", *IEEE Access*, Vol. 9 (May 2021), pp. 68376–68386.

50 Tianjiao Jiang, "The Shift of China's Strategic Thinking on Cyberwarfare Since the 1990s", *Journal of Chinese Political Science*, Vol. 28 (May 2022), pp. 136–141. Matthew J. Dagher-Margosian, "CCP Cyber Sovereignty Contains Lessons for AI's Future", *China Brief*, Vol. 24, Issue 8 (April 12 2024), https://jamestown.org/program/ccp-cyber-sovereignty-contains-lessons-for-ais-future/, accessed September 1 2024.

51 Thomas G. Mahnken, *Secrecy and Stratagem: Understanding Chinese Strategic Culture* (Double Bay, NSW: Lowy Institute for International Policy, 2011), p. 8.

52 Juliana Suess and Jack Crawford, "Russia and China Reaffirm Their Space Partnership" (April 12 2024), https://www.rusi.org/explore-our-research/publications/commentary/russia-and-china-reaffirm-their-space-partnership, accessed April 13 2024.

it remains to be seen how Sino-Russian cooperation will develop or whether this non-aggression pact will hold or be extended, but China seeks to maximize the benefits it believes it can draw from cyber as the fifth domain of warfare.[53] This discussion is returned to in the penultimate section.

3 From theory to practice: cyberespionage, pre-positioning, and holding critical infrastructure "at risk"

These cyber theorems helped guide and direct policy choices. Chapter 2 detailed how China was beginning to operationalize its theories and by the mid-2000s cyber recruitment and training programs were underway. Chinese hackers had begun infiltrating CI as early as 2001 and from September 2003-August 2005 "Titan Rain" intruded into Department of Defense laboratories, NASA networks, and aerospace companies. In 2007–2009, "Night Dragon" infiltrated the U.S. electric system to map and find ways to disrupt the grid, and also targeted oil, gas, energy, and petrochemical companies worldwide.

Night Dragon appears to have been run by APT1 ("Comment Crew") operating out of PLA Unit 61398 (which, amongst other things, has been long accused of targeting companies in CI). This included the Canadian branch of Spanish-based company Telvent, one of a number of supply chain and gateway companies to larger critical infrastructure providers.[54] In the early 2010s, "Operation Aurora" went after defense suppliers, including a prime contractor in Lockheed Martin. In addition, it targeted American merchant "shipping, aeronautics, arms, energy, manufacturing, engineering, electronics, financial, and … software companies" which included Yahoo and Google.[55]

Alongside this the "Shady Rat" campaign was running against a broad range of targets.[56] This was, like many other Chinese campaigns, primarily looking at intel-

53 Elsa B. Kania and John Costello, "Seizing the Commanding Heights: The PLA Strategic Support Force in Chinese Military Power", *Journal of Strategic Studies*, Vol. 44, No. 2 (March 2021), pp. 244–246.

54 David E. Sanger, David Barboza, and Nicole Perlroth, "Chinese Army Unit is Seen as Tied to Hacking Against U.S." (February 18 2013), https://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html, accessed May 8 2019.

55 Mark Clayton, "Stealing US Business Secrets: Experts ID Two Huge Cyber 'Gangs' in China" (September 14 2012), https://www.csmonitor.com/USA/2012/0914/Stealing-US-business-secrets-Experts-ID-two-huge-cyber-gangs-in-China, accessed April 26 2019.

56 Dmitri Alperovitch, "White Paper, Revealed: Operation Shady RAT: An Investigation of Targeted Intrusions into More Than 70 Global Companies, Governments, and Non-profit Organizations dur-

lectual property (IP) theft. Meanwhile, the 2013–2015 breach of the U.S. Office of Personnel Management was geared to gather details of American government employees. This provided Chinese intelligence with access and leverage to personnel and organizations directly tied to the U.S. government.

More broadly, tailored cyberattacks and attackers can also be bought or hired "off the shelf" to operate as privateers or proxies, and improving capabilities and practice have led to exponential quantitative growth and innovation. At the cost of a laptop and Internet connection the barriers to entry have continued to fall, with malware code and tools widely available and increasingly user friendly. Technical malware and code analysis is one of the main investigative pathways used to identify the attackers and their origins, but these are movable pieces in a dynamic global jigsaw.

This is reflected in Chinese APT campaigns with so-called "living-off-the-land" practices that use pre-existing or repurposed malware and open-source tools making attribution more challenging.[57] This said, discovery and "naming and shaming" individuals who operate as part of APT groups and identifying their physical location and infrastructure might well have been one of the reasons why the PRC has undergone two major restructures of its cyberespionage operations. Without significant changes it could have been more difficult for Chinese counterintelligence to protect and support them.[58]

Cyberespionage operations have been important to Chinese development. From 2000 to 2010 the PLA's campaigns saw China begin a two-fold leap. For military advancement, which was a significant focus for the PLA, IP theft and reverse engineering-appropriated technologies were instrumental in progressing the PLA from mechanized-age weapons to "an informationized force". Seen within Chinese culture as the sincerest form of flattery, IP theft also targeted civilian industries.[59] Civilian IP, with America the prime target, has been rapidly incorporated into Chinese products and bred material and economic development. By design, and with insufficient attention from national governments and private industry, the West

ing the Last Five Years" (2011), p. 6, http://www.csri.info/wp-content/uploads/2012/08/wp-operation-shady-rat1.pdf, accessed April 26 2019.

57 For example, malware can be modified and repurposed by other groups but has regularly been reused by the same or similar groups in multiple campaigns.

58 William Tsing, "The Advanced Persistent Threat Files: APT1" (February 22 2019), https://blog.malwarebytes.com/threat-analysis/2019/02/the-advanced-persistent-threat-files-apt1/, accessed November 1 2021.

59 Peter K. Yu, "The Second Coming of Intellectual Property Rights in China", Occasional Papers in Intellectual Property Law from Benjamin N. Cardozo School of Law Yeshiva University, No. 11 (2002), pp. 1–67.

and the rest have been hemorrhaging national and supranational science and technology and intelligence. Additionally, China's cyberespionage campaigns have also provided China's politico-military leadership with the ability to engage in disruptive or destructive cyberwarfare through pre-positioning in CI. This is a cause for concern. Chapter 2 outlines how and what they are pre-positioning against. This is part of the fourth industrial revolution (4IR/Industry 4.0) and wider discussions of disruptive technologies.

Chapter 2 also detailed the 2013 Science of Military Strategy which talked of the use of "privateer" forces and flagged the start of a process to centralize cyber operations under one body, the PLASSF. Under President Xi Jinping, China also set about reorienting its strategy for "Information Warfare" (read as cyberwar to many in the West) with the groundwork part of wider military reorganizations and reform (articulated in China's 2015 Military Strategy). Chapter 2 also discussed how these injections provided by cyberespionage – allied to the skills and knowledge base provided by China's universities and its large numbers of foreign students and staff working in Western universities and conducting business with the West – are allied to industry and state priorities.

Chapter 2 also noted that China is developing indigenous supercomputers, quantum computing and quantum encryption, Machine Learning, and AI. These are technologies that could well have profound implications for cyberespionage and the capacity to engage in cyberwarfare at scale. In these fields, China is engaged in a developmental race with the U.S. and the West more widely. Thus far, China has largely engaged in cyberespionage and targeted IP theft.

However, both in conventional approaches to espionage and in cyberspace, they have also gone directly and indirectly after companies and personnel involved in CI. Business leaders, officials, non-governmental and intergovernmental organizations, and universities have also all been targeted. In addition, companies including DJI, China General Nuclear Power Group, Huawei, and ZTE are all suspected of being potential vehicles for the CCP and PLA. Even as cost-effective and reliable providers there are widespread concerns over inviting Chinese companies into Western telecommunications and nuclear power (two key areas of critical infrastructure). More widely still, China is the world's pre-eminent manufacturer of microchips found in systems worldwide, and this also raises valid concerns.

Northrop Grumman's thorough 2012 study detailed state-sponsored or state-directed infiltration from China of the supply chains for microelectronics, including high-value targets such as defense and telecommunications. This includes the pos-

sibility of malicious chips or circuit boards, including for routers and switches and other fundamental hardware, having hidden features.[60]

This includes corrupting the Basic Input/Output System used to boot operating systems including Windows. These can be updated by vendors or by malware through watering-hole attacks (where a site likely to be visited by a particular target group is compromised) and other methods.[61] This applies also to firmware (code to enable functionality of hardware installed by manufacturers).[62] For this to happen these features would have to be designed into the manufacturing phase or developed to enable trojanized access through downstream suppliers. Northrop Grumman stated this "has the potential to cause a catastrophic failure of select systems and networks supporting critical infrastructure for national security or public safety".[63]

With evidence suggesting that cybersecurity risks are growing faster than the ability to secure data and systems from a wide variety of hostile actors from China and the rest of the world, the cybersecurity industry and government agencies, most notably the NSA, work under a considerable burden.[64] The Western Intelligence Community leans heavily on the cybersecurity industry and their threat prevention tools, mitigations, investigations, and analysis. They, and the private industry they protect, alongside Western governments (and many other nations), are now seeing threats on an unprecedented scale, and of unprecedented diversity and complexity, in cyberspace.

This has seen private industry and governments constantly trying to monitor, mitigate, or remediate vulnerabilities as well as attempts to infiltrate the communications and social relationships of target groups and individuals. This is global in

---

60 Bryan Krekel, Patton Adams, and George Bakos, *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage*, prepared for the U.S.–China Economic and Security Review Commission by Northrop Grumman Corp. (McLean, VA: Northrop Grumman Corporation, March 7 2012), pp. 11–12, https://info.publicintelligence.net/USCC-ChinaCyberEspionage.pdf, accessed April 16 2019.

61 Wang Zhengde, Yang Shisong, and Zhou Lin (eds.), *Xinxi Duikang Lilun* (*Information Confrontation Theory*) (Beijing: PLA Information Engineering University/ Military Science Publishing House, 2007), p. 208.

62 Cassius Puodzius, "UEFI Malware: How to Exploit a False Sense of Security" (October 19 2017), https://www.welivesecurity.com/2017/10/19/malware-firmware-exploit-sense-security/, accessed April 16 2019.

63 Krekel, Adams, and Bakos, *Occupying the Information High Ground*, p. 12.

64 David Chinn, James Kaplan, and Allen Weinberg, "Risk and Responsibility in a Hyperconnected World: Implications for Enterprises" (undated), http://www.mckinsey.com/insights/business_technology/risk_and_responsibility_in_a_hyperconnected_world_implications_for_enterprises, accessed February 15 2016.

scope. The range of state-, sub-state-, and non-state-level threats is wide and deep, with Russia, Iran, North Korea, and counterterrorism high on the list. At the top of that list is the PRC. However, chapter 2 concludes that China is also potentially vulnerable because of Western components (as well as firmware and software) in China's industrial critical infrastructure. How they might deal with a potential major cyberattack on their CI concerns them also.

These threats emanate from individuals and groups who are often well organized. If these are privateer or proxy forces, they are frequently in locations where extradition is a problem. If they are state-level actors working for intelligence agencies, operatives are not going to be extradited. This includes those operating in China. A visit to the FBI "Cyber's Most Wanted" page reveals a string of indictments and arrest warrants against Chinese nationals (as well as many other nations – especially Russia, Iran, and North Korea).[65] However, then FBI Director Christopher Wray testified in January 2024 that Chinese cyber threats are greater "than every other major nation combined".[66] Wray attested:

> the PRC's cyber onslaught goes way beyond prepositioning for future conflict. Today, and literally every day, they're actively attacking our economic security – engaging in wholesale theft of our innovation and our personal and corporate data ... they knit cyber into a whole-of-government campaign against us. They recruit human sources to target our businesses, using insiders to steal the same kinds of innovation and data their hackers are targeting while also engaging in corporate deception – hiding Beijing's hand in transactions, joint ventures, and investments – to do the same.[67]

Then-White House national cyber Director, Harry Coker, Japan's Deputy National Security Advisor, Keiichi Ichikawa, and Britain's Director of GCHQ, Anne Keast-Butler, raised very similar concerns.[68]

---

65 "Cyber's Most Wanted", https://www.fbi.gov/wanted/cyber, accessed October 9 2021.

66 Christopher A. Wray, Director, Federal Bureau of Investigation, Washington, D.C., "Opening Statement" (January 31 2024), https://www.fbi.gov/news/speeches/director-wrays-opening-statement-to-the-house-select-committee-on-the-chinese-communist-party, accessed March 4 2024.

67 Christopher A. Wray, Director, Federal Bureau of Investigation, Washington, D.C., "Opening Statement" (January 31 2024).

68 Mickey Carroll, "GCHQ Boss Says China's 'Genuine' Cyber Threat 'Weakens Security of Internet For All'" (May 14 2024), https://news.sky.com/story/gchq-boss-says-chinas-genuine-cyber-threat-weakens-security-of-internet-for-all-13135724, accessed May 14 2024.

4 China: a cyber threat, a rising power, and an opportunity to engage

Chinese cyberespionage poses a major concern in the context of U.S. innovation through IP theft. This includes military systems technology. This was the subject of chapter 3. The head of MI5, Britain's domestic counterintelligence agency, in a joint statement with FBI Director Wray, outlined in July 2022 how China has been conducting "a coordinated campaign on a grand scale … a strategic contest across decades … [through] planned, professional activity".[69] Michael J. Rogers, then Chair of the House (Select) Intelligence Committee, had earlier stated in 2014:

> I called out the Chinese government for its industrial-scale campaign of cybereconomic espionage against American companies. The brazen Chinese government campaign was no secret in the United States government or the private-sector cybersecurity community. But no one was talking about it publicly at that time. The United States was unwilling to call Beijing to account, and U.S. companies feared the Chinese government would punish them with crushing cyberattacks for having that public debate. After we opened that debate here and called China out, we were able to have an honest conversation with the American people about the cost of this Chinese campaign and what needs to be done about it. China's economic cyberespionage has certainly not diminished in that time. In fact, it's grown exponentially in terms of volume and damage done to our nation's economic future. Chinese intelligence services that conduct these attacks have little fear, because we have no practical deterrence to that theft. This problem is not going away until that changes.[70]

Little has changed and Chinese cyberespionage impacts much more than America's economic future. A late 2018 congressional commission warned that America was falling behind in areas such as AI and hypersonic platforms. Falling behind in these critical advanced technologies "raises the possibility that America may find itself at a technological disadvantage in future conflicts".[71] The commission added, "Because the American way of war has long relied on technological supremacy, this could have profoundly negative implications for U.S. military effectiveness".[72]

---

69 Joint Address by MI5 and FBI Heads (July 6 2022), https://www.mi5.gov.uk/news/speech-by-mi5-and-fbi, accessed March 18 2024.

70 "Hearing of the House (Select) Intelligence Committee Subject: 'Cybersecurity Threats: The Way Forward' (November 20 2014), https://www.nsa.gov/news-features/speeches-testimonies/Article/1620360/hearing-of-the-house-select-intelligence-committee-subject-cybersecurity-threat/, accessed January 16 2019.

71 In turn this might provide greater impetus for America and the West to conduct their own espionage in these areas. "Providing for the Common Defense: The Assessment and Recommendations of the National Defense Strategy Commission" (2018), p. 10, https://www.usip.org/publications/2018/11/providing-common-defense, accessed December 20 2018.

72 "Providing for the Common Defense", p. 10.

Resultantly, it can be argued that this makes it more likely that the United States will come under challenge, with knock-on effects for friends and allies, especially in NATO and the Asia-Pacific. One of America's strengths from 1941 onwards has been in alliances. Notwithstanding changes in U.S. foreign and defense policy that might emerge under the second Trump administration, China's demographic and geographic size, alongside its economic weight and relative state cohesiveness enforced by the CCP, portend that "quantity exhibits a quality all its own".[73]

Given that America far outspends China on defense, they are looking to maintain the military advantages they have held since World War II. However, what is not being factored in is how much China has saved on R&D through cyberespionage against the U.S. defense-industrial base and related sectors. As China has moved into priority areas of R&D across a range of developing and Emerging Technologies, and from development into testing and evaluation it has moved into second place in the list of global defense expenditure.[74]

In 2021 China's official defense budget was ¥1.355 trillion (renminbi/yuan). That equated to around $209 billion USD.[75] In 2022, it was ¥1.45 trillion ($229 billion).[76] By 2023, it had risen to ¥1.55 trillion (around $243 billion).[77] These are official Chinese government figures. The widely respected Stockholm International

73 Timothy L. Thomas, *Three Faces of the Cyber Dragon: Cyber Peace Activist, Spook, Attacker* (Fort Leavenworth, KS: Foreign Military Studies Office, 2012), p. 157.

74 Testing and evaluation is necessary before commissioning systems into combat duty. Nan Tian and Fei Su, "A New Estimate of China's Military Expenditure" (January 2021), https://www.sipri.org/sites/default/files/2021-01/2101_sipri_report_a_new_estimate_of_chinas_military_expenditure.pdf. "World Military Spending Rises to Almost $2 Trillion in 2020" (April 26 2021), https://www.sipri.org/media/press-release/2021/world-military-spending-rises-almost-2-trillion-2020. Both accessed November 8 2021.

75 Campbell, "China's Military: The People's Liberation Army", p. 47.

76 Amrita Jash, "China's 2022 Defense Budget: Behind the Numbers" (April 29 2022), https://jamestown.org/program/chinas-2022-defense-budget-behind-the-numbers/, accessed November 8 2024.

77 Amrita Jash, "China's 2023 Defense Spending: Figures, Intentions and Concerns", *China Brief*, Vol. 23 Issue 7 (April 14 2023), https://jamestown.org/program/chinas-2023-defense-spending-figures-intentions-and-concerns/. Nan Tian, Diego Lopes da Silva, Xiao Liang, and Lorenzo Scarazzato, "Trends in World Military Expenditure, 2023" (April 2024), https://www.sipri.org/sites/default/files/2024-04/2404_fs_milex_2023.pdf. Both accessed November 14 2024. SIPRI's estimate is 1.7–1.9 percent of GDP. Nan and Fei, "A New Estimate of China's Military Expenditure", p. 18.

Peace Research Institute's last estimated figure was higher at $296 billion for 2023. This was a 6 percent rise and the 29th year-on-year rise.[78]

In June 2023 U.S. Senate hearings it was revealed that the U.S. Intelligence Community (USIC) assessed PRC defense spending might be nearer $700 billion.[79] Publicly declared budgets are one thing. Real defense spending is another.[80] Sectoral and general inflation is also a factor. The U.S. defense budget request for FY2024 was far in excess of China's at $849.8 billion. Of that, $143 billion is for research, development, testing, and evaluation (RDT&E).[81] Past expenditure on RDT&E has benefitted the PRC/PLA. How much of the 2024 budget and future expenditure will indirectly benefit China because of cyberespionage?

As chapter 3 detailed, the aerospace sector and other parts of the defense-industrial base have been widely and successfully targeted. Based on the sectors and some of the companies China has successfully targeted, chapter 4 detailed how China has used cyberespionage to grow, accelerate, and develop its military capabilities across the spectrums of land, air, sea, and space. This includes heavy-lift airplanes, fourth- and fifth-generation multi-role aircraft, and missiles. Western R&D might well have shortened China's pathways to reverse engineering and manufacturing. This includes "Chinese copies" of Western aircraft like the Chengdu J-20 "Mighty Dragon", Shenyang J-31 "Gyrfalcon", and the Xi'an Y-20.

Chapter 4 also detailed how the PRC has developed and deployed "carrier-killer" missiles, a new series of short-, intermediate-, and intercontinental-range ballistic missiles. This includes difficult-to-defend-against Mach 5+ hypersonic missiles, including antiship cruise missiles. Antiship missiles have been installed on the Spratly and Paracel island archipelagos and surface-to-air missiles on artificial reefs in the "first island chain" stretching across the Philippines Sea. This has been developed into a protective net for the PLAN in the South China Sea, a barrier to entry for Western navies, notably the USN and allied forces (especially for the possible defense of Taiwan), and a potential staging post in the Western Pacific.[82] It

78 "Global Military Spending Surges Amid War, Rising Tensions and Insecurity" (April 22 2024), https://www.sipri.org/media/press-release/2024/global-military-spending-surges-amid-war-rising-tensions-and-insecurity, accessed November 8 2024.

79 Caitlin Campbell, "China Primer: The People's Liberation Army (PLA)" (September 16 2023), https://crsreports.congress.gov/product/pdf/IF/IF11719, accessed November 8 2024.

80 Peter E. Robertson, "The Military Rise of China: The Real Defence Budget Over Two Decades", *Defence and Peace Economics*, Vol. 35, No. 7 (2024), pp. 809–825.

81 Jim Garamone and C. Todd Lopez, "DOD's 2025 Budget Request Provides 4.5% Raise for Service Members" (March 11 2024), https://www.defense.gov/News/News-Stories/Article/Article/3703751/dods-2025-budget-request-provides-45-raise-for-service-members/, accessed November 8 2024.

82 "Military and Security Developments Involving the People's Republic of China 2022", Annual Report to Congress, pp. VIII, 57, 64–65, 83, https://media.defense.gov/2022/Nov/29/2003122279/-1/-1/1/

has also employed lawfare in territorial disputes in the South China Sea (reflecting neoclassical realism).[83]

In addition, China has also been testing and developing anti-satellite missiles since 2007. These capabilities are supported by airborne early-warning aircraft and antisubmarine warfare systems (especially hunter-killer submarines). These are integrated into wider C4ISR assets. This includes constellations of Chinese satellites. These all form part of Chinese anti-access/area-denial capabilities and strategies. At sea, the Department of Defense recognizes that the PLAN now exceeds the USN. By 2025, the PLAN is expected to grow to 395 vessels. By 2030, that number is expected to be 425.[84]

Partly to counter China's PLAN, as of 2024 the USN is planning on a force of 294–296 "battle force ships" by 2030 whilst increasing the percentage of its fleet to the Pacific. This includes its newest and most capable vessels. In 2021, what was envisaged for the USN was a smaller portion of larger ships, a larger portion of smaller ships, and a substantially greater use of unmanned vehicles and shifting a greater proportion of its fleet to the Pacific as part of a regional focus or "pivot to Asia".[85] The shift to the Pacific remains for now. In addition, the policy of the Biden administration also meant increasing:

> cooperation with naval forces from allies such as Japan and Australia and other countries such as India, including exercises and other forms of engagement … aimed not only at improving interoperability between U.S. and allied naval forces, but also at expanding existing bilateral forms of naval cooperation (e.g., U.S.–Japan, U.S.–Australia, U.S.–India) into trilateral (e.g., U.S.–Japan–Australia, U.S.–Australia–India) or quadrilateral (U.S.–Japan–Australia–

2022-MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA.PDF, accessed November 9 2024.

83 Douglas Guilfoyle, "The Rule of Law and Maritime Security: Understanding Lawfare in the South China Sea", *International Affairs*, Vol. 95, Issue 5 (September 2019), pp. 999–1017. Huiyun Feng and Kai He, "A Dynamic Strategic Culture Model and China's Behaviour in the South China Sea", *Cambridge Review of International Affairs*, Vol. 34, No. 4 (2021), pp. 510–529.

84 Campbell, "China's Military: The People's Liberation Army", p. 30. See also Brent D. Sadler, *U.S. Naval Power in the 21st Century: A New Strategy for Facing the Chinese and Russian Threat* (Annapolis, MD: U.S. Naval Institute Press, 2023) and Michael A. McDevitt, *China as a Twenty-First Century Naval Power: Theory, Practice, and Implications* (Annapolis, MD: U.S. Naval Institute Press, 2023).

85 The original version of this document dated October 7 2021 spoke of the USN plans to expand from 308 to 355 vessels and developing "a once-in-a-generation change in fleet architecture". Ronald O'Rourke, "China Naval Modernization: Implications for U.S. Navy Capabilities – Background and Issues for Congress" (August 16 2024), pp. 35–37, 51, https://sgp.fas.org/crs/row/RL33153.pdf, accessed November 9 2024. Relatedly, U.S. defense contractors are developing a Long-Range Anti-Ship Missile and Advanced Anti-Radiation Guided Missile, as well as planning force modernization including a DDG(X) Next-Generation Destroyer Program and Next-Generation Attack Submarine. O'Rourke, "China Naval Modernization: Implications for U.S. Navy Capabilities", pp. 51–52."

> India) forms that could enhance the ability of the United States and its allies in the Indo-Pacific region to balance against China's growing military capabilities and deter potential assertive actions by China.[86]

Cooperative agreements alleviate some concerns of overstretch, with America the keystone of NATO and with interests and allies in the Middle East and South Asia. The second Trump administration might take a different view of U.S. alliances and regional allies. This is a foreign and defense policy choice.

Under the Biden administration the U.S. entered into a trilateral security partnership with the UK and Australia (AUKUS). This saw Australia cancel a $90AUD billion contract with the French government for 12 SSNs (attack submarines), and instead Australia planned to purchase at least eight SSNs built in Australia through a build and refit program with the U.S. and UK. AUKUS is designed to encompass "diplomatic, security and defence co-operation in the Indo-Pacific. This includes joint work on cyber capabilities, AI, quantum technologies and 'additional undersea capabilities', such as underwater sensors and drones".[87] Whether to continue AUKUS will be another policy choice.

Across the range of physical domains of land, sea, and air, America still remains at or near the top of global rankings in numerical terms.[88] Comparing raw numbers does not account for equipment quality, interoperability, jointness between service branches, availability of supplies, logistics, or many other warfighting factors. There are also parameters that are not easily measured. These include training, operational and combat experience, and morale (key aspects of

---

86 O'Rourke, "China Naval Modernization: Implications for U.S. Navy Capabilities", pp. 53–54.

87 Anonymous, "Australia is Getting Nuclear Subs, with American and British Help. The New AUKUS Alliance Reflects a Shared Fear of China" (September 15 2021), https://www.economist.com/asia/australia-is-getting-nuclear-subs-with-american-and-british-help/21804790. Valerie Niquet and Marianne Peron-Doise, "AUKUS and Submarines: The Fallout for France" (September 18 2021), https://thediplomat.com/2021/09/aukus-and-submarines-the-fallout-for-france/. Felix K. Chang, "Strategic Choice: Australia's Nuclear-Powered Submarines" (October 21 2021), https://www.fpri.org/article/2021/10/strategic-choice-australias-nuclear-powered-submarines/. Arzan Tarapore, "AUKUS Is Deeper Than Just Submarines" (September 29 2021), https://fsi.stanford.edu/news/aukus-deeper-just-submarines. Reuters and Angus Watson, "France's Macron Says Australian Prime Minister Lied to Him on Submarine Deal" (November 1 2021), https://edition.cnn.com/2021/10/31/australia/macron-morrison-australia-france-submarine-deal-intl-hnk/index.html. Media Statement (September 16 2021), https://www.pm.gov.au/media/australia-pursue-nuclear-powered-submarines-through-new-trilateral-enhanced-security. All accessed November 7 2021. It is noteworthy that through cyberespionage, China has gained details of U.S. and allied weapons systems which might well be providing the PLA with the ability to develop and deploy countermeasures.

88 "United States Military Strength" (undated), https://www.globalfirepower.com/country-military-strength-detail.asp?country_id=united-states-of-america, accessed January 16 2020.

warfighting for Clausewitz and Sun Tzu). In these areas, and supported by like-minded nations and long-standing allies and friends, America is believed to still possess clear advantages.

Cooperative agreements include intelligence sharing through the "Five Eyes" partnership, and bilateral and multilateral intelligence-sharing arrangements. This includes cyber threat intelligence sharing. Cyberespionage, through to the threshold into cyberwarfare, can undercut qualitative vs. quantitative advantages, making asymmetries appear larger than they might be. This might make China much closer to parity in conventional forces than is often thought should it begin hard-power contestation and enter the realm of "Thucydides' Trap".[89] China also remains a capable nuclear power with SSBNs and land-based missiles, and a small number for air-delivery by Xian H-6 bombers. These nuclear capabilities could grow.[90] This, too, is part of the security dilemma.[91]

There are also wider considerations that impact the security dilemma. If it were possible to aggregate all that China has accrued through cyberespionage, across military *and* civilian sectors, these numbers would be eyewatering. There are crumbs of comfort as "Chinese scholars argue that China's defense budget – which the PRC presents as insufficient to meet China's defense needs – will need to expand to unsustainable levels as the PLA replaces legacy systems with more modern and expensive ones".[92] However, China is also finding export markets for its military products, as it does across the civilian sector. In 2019, 8 of the world's 25 largest defense contractors were state-owned Chinese firms.[93] These are listed in table 1:

---

89 "Key Trends across a Maturing Cyberspace Affecting U.S. and China: Future Influences in a Rising Deeply Cybered, Conflictual, and Post-Western World; Dr. Chris C. Demchak Testimony before Hearing on China's Information Controls, Global Media Influence, and Cyber Warfare Strategy Panel 3: Beijing's Views on Norms in Cyberspace and China's Cyber Warfare Strategy, U.S.–China Economic and Security Review Commission, Washington, DC, 4 May 2017", p. 17, https://www.uscc.gov/sites/default/files/Chris%20Demchak%20May%204th%202017%20USCC%20testimony.pdf, accessed April 3 2020.

90 Tong Zhao, "China's Strategic Arsenal: Worldview, Doctrine, and Systems" (December 2021), https://www.armscontrol.org/act/2021-12/arms-control-today/chinas-strategic-arsenal-worldview-doctrine-systems?mkt_tok=MDk1LVBQVi04MTMAAAGBHAcG6p6XxDhpXxaTULXp3VBv1F9X4VjKd3aHSBScTgLENhTE1fa2qeM5FBoz7kq51iTj2SDlTsFHEzNA3_TmyYOUuuRRHoKWWSrvl8bJ3I8FKw, accessed December 4 2021.

91 Robert Jervis, "Cooperation Under the Security Dilemma", *World Politics*, Vol. 30, No. 2 (January 1978), pp. 167–214.

92 There is also a growing synergy between civilian and military sectors aided by dual-use technologies such as semiconductors, software, and emerging technologies. Campbell, "China's Military: The People's Liberation Army", pp. 48–49.

93 Campbell, "China's Military: The People's Liberation Army", p. 50.

Table 1: Global Rankings of China's Top Defense State-Owned Companies in 2019

Company	Defense News ranking (out of 100)	Stockholm International Peace Research Institute ranking (out of 25)
Aviation Industry Corporation of China (AVIC)	6	6
China North Industries Group Corporation Limited (NORINCO)	8	9
China Aerospace Science and Industry Corporation (CASIC)	11	Not ranked
China Shipbuilding Industry Corporation (CSIC)	14	Not ranked
China Electronics Technology Group Corporation (CETC)	15	8
China South Industries Group Corporation (CSGC)	18	24
China Aerospace Science and Technology Corporation (CASC)	20	Not ranked
China State Shipbuilding Corporation (CSSC)	24	Not ranked
China National Nuclear Corporation (CNNC)	Not ranked	Not ranked

Source: Caitlin Campbell, China's Military: The People's Liberation Army (PLA), p. 51, https://crsreports.congress.gov/product/pdf/R/R46808, accessed November 8 2021.

Trade imbalances between the U.S. and China were an important part of economic policy during the first Trump administration. This is one of the policy areas that could be revisited as part of Sino-U.S. engagement under the second Trump administration. More widely, the post-World War II liberal order has been enabled through security pacts, tariff-free (or non-protectionist) trade, and multilateral rules and institutions, alongside strategic partnerships (especially NATO) binding together advanced industrial democracies under the umbrella of American leadership and power. Whether these sets of imperatives are important to a more inward-looking, America-first, second Trump administration remains a concern.[94]

94 William Mathews, "Trump's 'America First' Foreign Policy will Accelerate China's Push for Global Leadership" (November 14 2024), https://www.chathamhouse.org/2024/11/trumps-america-first-foreign-policy-will-accelerate-chinas-push-global-leadership, accessed November 30 2024.

This could produce a separate and rival, hegemonic order to liberal internationalism and lead to international instability and unstable friendships and alliances.[95] This also depends on whether a risen China seeks to work within the existing international order, challenges it, or seeks to overturn it.[96] This includes issues relating to the "cyber order", involving technical standards, future developments of the Internet (with concerns over national "Splinternets"), and supporting technologies.[97]

On trade, and in other cooperative areas, whether China will seek new global rules and institutions or whether it will work within the existing Western-led international order, and how that order might be challenged from within and without, is a complex international and globally impactful dynamic.[98] China is, after all, deeply rooted in the international system, both through global institutions, including the United Nations Security Council, large intergovernmental organizations including BRICS, the World Trade Organization, and G20 whilst in areas involving human rights it contests issues resulting from its one-China policy amid accusations of repression and coercion.[99]

It is also often the biggest player in regional organizations like the Shanghai Cooperation Organization (SCO), Shangri-La Dialogue, Asian Infrastructure Investment Bank, and Association of South-East Asian Nations through economic weight as it has risen to upper-middle-income status among developed nations whilst becoming the largest creditor for developing nations. This has been described as

---

95 Darren J. Lim and G. John Ikenberry, "China and the Logic of Illiberal Hegemony", *Security Studies*, Vol. 32, No. 1 (2023), pp. 1–31. G. John Ikenberry, "The Rise of China and the Future of the West: Can the Liberal System Survive?", *Foreign Affairs*, Vol. 87, No. 1 (January/February 2008), pp. 23–37.

96 Amy King, "The Collective Logic of (Chinese) Hegemonic Order". Matthew D. Stephen, "China and the Limits of Hypothetical Hegemony". Darren J. Lim and G. John Ikenberry, "China and Hegemony: An Exchange – The Authors Reply". All in *Security Studies*, Vol. 33, No. 1 (2024), pp. 146–164.

97 Mallick, *China in the Cyber Domain*, pp. 365–405. Bruno Lété, "The Paris Call and Activating Global Cyber Norms", German Marshall Fund of the United States (2021), https://www.jstor.org/stable/pdf/resrep30240.pdf, accessed December 13 2024.

98 Lim and Ikenberry, "China and the Logic of Illiberal Hegemony", pp. 1–31. Mathew D. Stephen, "China's New Multilateral Institutions: A Framework and Research Agenda", *International Studies Review*, Vol. 23, Issue 3 (September 2021), pp. 807–834.

99 Yao Li and Manfred Elfstrom, "Does Greater Coercive Capacity Increase Overt Repression? Evidence from China", *Journal of Contemporary China*, Vol. 30, Issue 128 (2021), pp.186–211. Han Zhu and Lu Jun, "The Crackdown on Rights-Advocacy NGOs in Xi's China: Politicizing the Law and Legalizing the Repression", *Journal of Contemporary China*, Vol. 31, Issue 136 (2022), pp. 518–538. Edward Lemon, Bradley Jardine, and Natalie Hall, "Globalizing Minority Persecution: China's Transnational Repression of the Uyghurs", *Globalizations*, Vol. 20, Issue 4 (2023), pp. 564–580.

"contested multilateralism".[100] This is in evidence through some ongoing efforts by China to create new institutions within multilateral frameworks. However, this pursuit tends to be only undertaken as a strategy of "last resort" when existing forums and "forum shopping" have been exhausted as options.[101]

Beyond trade and institutional pressure, there are a multiplicity of other areas where American engagement with their Chinese counterparts might serve as a better deterrent to cyberespionage than under previous administrations. This, too, is a policy choice. Another is arms control. Whether conventional or unconventional, this is an available option Under the Reagan administration, arms control with the Soviet Union was pursued whilst ramping up conventional and nuclear force modernization. Both policies were successful legacies of his administration. These deals benefitted America and global security. Whilst capping numbers and the deployment of classes of weapons, the cost of arms racing America drained the Soviet economy and was a contributor to the eventual collapse of the USSR between 1989 and 1991[102]

One of the lessons Reagan took into his second term of office was that successful negotiation required reaching out and finding accommodation with America's key adversaries as well as with America's allies and friends around the world.[103] That system of alliances has helped keep the peace since World War II. Soft power was, and remains, another important aspect of the *Rise and Fall of the Great Powers.*[104] Differing systems of government, challenges to liberal democracy, and a return to great power competition are also features that could once more provoke a *Clash of Civilizations.*[105] Alongside economic competition, cultural exchanges and

100 Julia C. Morse and Robert O. Keohane, "Contested Multilateralism", *Review of International Organizations*, Vol. 9, No. 4 (December 2014), pp. 385–412.

101 Stephen, "China's New Multilateral Institutions", pp. 807–834.

102 For debate around these issues see James Mulvenon, Didi Kirsten Tatlow, and Alex Joske, "Mitigation Efforts to Date", in William C. Hannas and Didi Kirsten Tatlow (eds.), *China's Quest for Foreign Technology: Beyond Espionage* (New York: Routledge, 2021), pp. 307–327.

103 Paul Nitze, *From Hiroshima to Glasnost: At the Center of Decision – A Memoir* (with Ann M. Smith and Steven L. Rearden) (New York: Grove Weidenfeld, 1989). David Reynolds, *Summits: Six Meetings That Shaped the Twentieth Century* (London: Allen Lane, 2007), pp. 317–369.

104 Paul Kennedy, *Rise and Fall of the Great Powers: Economic Change and Military Conflict from 1500–2000* (New York: Random House, 1988).

105 Samuel P. Huntingdon, "The Clash of Civilizations", *Foreign Affairs*, Vol. 72, No. 3 (Summer 1993), pp. 22–49. Samuel P. Huntingdon, *The Clash of Civilizations and the Remaking of World Order* (New York: Simon & Schuster, 1996). Samuel P. Huntingdon, "The Clash of Civilizations Revisited", *New Perspectives Quarterly*, Vol. 30, Issue 4 (October 2013), pp. 46–54.

immigration/migration are part of these challenges. China's approach also chimes with Nye's smart power framework.[106]

5 China's universities and private sector

Part of the reason for China's rise and ability to exploit cyberespionage lies in China's university sector. Further substantiating points made in chapter 1, China's civilian universities, their indigenous and international research, and their student–staff exchanges are also seen by the CCP and PLA as supporting the national effort in cyber and broader technological development. Nine of their universities – Fudan University, Harbin Institute of Technology, Nanjing University, Peking University, Shanghai's Jiao Tong University, Tsinghua University, Xi'an Jiaotong University, Zhejiang University, and the University of Science and Technology of China (USTC) – are a selective group designated as the C9 League. These elite universities receive 10 percent of China's national research budget. Corresponding to the Ivy League in the United States, the C9 League was established by two CCP Directives – Project 211 (1995) and Project 985 (1998) – "to raise the research standards of China's top universities".[107]

USTC in Hefei (Anhui Province) in eastern China is home to the Institute of Advanced Technology, University of Science and Technology of China. This is an important center for innovation in China. It is unique in operating two national laboratories, the National Synchrotron Radiation Laboratory, and the Hefei National Laboratory for Physical Sciences at the Microscale. It conducts fundamental scientific research and describes itself as a world leader in areas including quantum technologies, nanotechnology, high-temperature superconductivity, speech processing, and the life sciences. It also promotes technology transfer with the ICT industry and innovation in microelectronics, materials science, and quantum information (part of quantum science). It recruits within the top 0.3–0.5 percent of high school graduates.[108]

---

106 Joseph S. Nye, Jr., "Get Smart: Combining Hard and Soft Power", *Foreign Affairs* (July/August 2009), https://www.foreignaffairs.com/articles/2009-07-01/get-smart, accessed December 13 2024. Christian C. Madubuko and Chamunorwa Chitsungo, "The Evolution of China's Cyber-espionage Tactics: From Traditional Espionage to AI-Driven Cyber Threats against Critical Infrastructure in the West", *American Journal of International Relations*, Vol. 9, Issue 4 (2024), pp. 25–50.

107 "Best Universities in China 2019" (October 1 2018), https://www.timeshighereducation.com/student/best-universities/best-universities-china, accessed March 1 2019.

108 "UTSC Introduction", https://en.ustc.edu.cn/2011/0113/c5394a50095/page.htm, accessed March 1 2019.

Shanghai's Jiao Tong University is where China's political and business elite go to study. It has relationships with several of the world's top universities. It has produced much-in-demand technical engineers who go on to work for domestic and foreign multinationals. It too has partnered with elite universities abroad. Members of Jiao Tong University have co-authored research papers with members of PLA Unit 61398, including on issues of cyberwarfare and joint papers on network security and attack detection. Jiao Tong is also one of a number of Chinese universities to have established joint ventures with Western universities. This has included the University of Michigan and Carnegie Mellon University in Pittsburgh.[109]

Twelve universities in China have information security courses. All but two are public universities; the two others are the National University of Defense Technology and the PLA Information Engineering University.[110] Under the banner of "Education is not indoctrination", the School of Cyber Science and Engineering at Jiao Tong was China's "first university department that serves as a national talents training base in the field of information security".[111] In addition, China has sent over 1,700 PLA members to over 50 nations for study. The PRC has also hosted over 10,000 foreign military staff at military educational institutions across China. These link-ups include 38 with Russia, 29 with Pakistan, 21 with Thailand, and 25 with the United States between 2003 and 2016.[112]

There are long-standing concerns that Chinese academia are leveraging Western universities. For many years Chinese students have frequently made up a lucrative and significant part of the student intake. The Australian Strategic Policy Institute (ASPI) reported in 2018 that since 2007 over 2,500 Chinese academics with links to the PLA have worked at a wide number of Western universities. The most popular are in the United States, Australia, the United Kingdom, and Germany. There Chinese academics have worked in "strategic and emerging technology sectors such as quantum physics, signal processing, cryptography, navigation technology and autonomous vehicles".[113] This was described by China's PLA Daily as "picking flowers in foreign lands to make honey in China".[114]

---

109 Melanie Lee, "Top China College in Focus with Ties to Army's Cyber-spying Unit" (March 24 2013), https://www.reuters.com/article/net-us-china-cybersecurity-university/top-china-college-in-focus-with-ties-to-armys-cyber-spying-unit-idUSBRE92N01120130324, accessed March 1 2019.

110 "2015 Top 12 Information Security Universities in China", https://www.cucas.edu.cn/studyinchina/top/2015_Top_12_Information_Security_Universities_in_China_1137-Hot_Rankings.html, accessed March 8 2019.

111 http://infosec.sjtu.edu.cn/en.php, accessed March 8 2019.

112 Campbell, "China's Military: The People's Liberation Army", p. 44.

113 Alex Joske, "Picking Flowers, Making Honey: The Chinese Military's Collaboration with Foreign Universities", ASPI International Cyber Policy Centre, Policy Brief Report No. 10/2018, p. 4,

In studying abroad, including PhD research and staff appointments, it has been suggested many academics retain "a strict loyalty to their government and the Chinese Communist Party".[115] Nationalism, and less party loyalty, might also play its part. Some have used cover stories ("legends") to mask their PLA affiliations.[116] London's *Times Higher Education* also reported on the ASPI research. It indicated not only the pre-pandemic scale of the Thousand Talents Plan, but also some of the anxieties it was provoking. There is sensitivity around the issue and even before the Covid-19 pandemic, leading researchers were being encouraged to return. There were also reports of FBI investigations.[117] To what extent this is a national security issue, rather than one of global mobility, remains a difficult question.[118] This especially concerns fundamental research in areas of strategic interest to the state. Penalizing entire groups based on their nationality is xenophobic. However, there are causes for concern as well as the well-evidenced FBI indictments.[119]

Though there are valid concerns, there is a great risk of tainting all Chinese students, academics, and businesspeople on this basis.[120] University research (both civilian and military) is utilized in the commercial sector and for military applications. Moreover, multinationals like Huawei and ZTE have long been believed to share with government intelligence collected from the West. Additionally, China is aiming to overtake the U.S. as the lead innovator of AI by 2030. Attempts are also underway to bridge the estimated deficit of 1.4 million trained cybersecur-

---

https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2018-10/Picking%20flowers%2C%20making%20honey_0.pdf?H5sGNaWXqMgTG_2F2yZTQwDw6OyNfH.u, accessed April 22 2019.

114 Wang Zhanwen and Zhu Qifeng, "Going Abroad, the Party Organization Life "Does Not Drop'" (July 1 2015), http://dangjian.people.com.cn/n/2015/0701/c117092-27237158.html, accessed July 1 2019.

115 Ben Westcott, "Chinese Army Scientists Exploiting Western Universities, Report Says" (October 1 2018), https://edition.cnn.com/2018/10/30/australia/pla-china-research-intl/index.html, accessed March 1 2019.

116 Westcott, "Chinese Army Scientists Exploiting Western Universities, Report Says".

117 John Morgan, "Western Universities Urged to Rethink Chinese Military Ties" (November 8 2018), https://www.timeshighereducation.com/news/western-universities-urged-rethink-chinese-military-ties, accessed March 1 2019.

118 Nigel Inkster, "The Chinese Intelligence Agencies: Evolution and Empowerment in Cyberspace", in Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron (eds.), *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain* (New York: Oxford University Press, 2015), pp. 34–37.

119 https://www.justice.gov/opa/pr/four-chinese-nationals-working-ministry-state-security-charged-global-computer-intrusion (July 19 2021), accessed October 16 2021.

120 Alex Joske, "How the West's Research Aids China's Military" (October 30 2018), https://www.aspistrategist.org.au/how-the-wests-research-aids-chinas-military/, accessed March 1 2019.

ity professionals needed by China as part of an "Assassin's Mace" (杀手链) ecosystem of research and training centers.[121]

6 Intelligence and counterintelligence

Back in 2012 Peter Mattis, a former counterintelligence analyst with the CIA, raised concerns about the scale of Chinese cyberespionage. At the time he questioned whether this was making its way to Chinese intelligence and the Chinese government. Mattis felt there was insufficient open-source intelligence/information to prove this conclusively.[122] This might still be so in some cases, but there is now enough open-source information to analyze Chinese cyberespionage and to show the scale of Chinese intelligence activities and how intelligence collection is being used by the Chinese government, the PLA, and in industries crucial to the CCP's Five-Year Plans.[123] Although much remains hidden, including detailed thinking and strategizing, the targets, military programs, and some of the civilian sectors which have benefitted from cyberespionage are clear. Offensively, through cyber and traditional espionage, one of China's main objectives has been to access the designs of Western (mainly American) military systems.

This is one of the reasons the U.S. founded the Office of Tailored Access Operations at the NSA's headquarters in Fort Meade in 1997. Through to 2012, this is said to have been very effective at penetrating Chinese computer and telecommunications systems and providing intelligence to the USIC.[124] What inroads have continued to be made is unclear, especially after the Snowden leaks and the uncovering of a major CIA spy operation in 2010–2012 (which involved physical break-ins to

121 Dakota Cary, "China's National Cybersecurity Center: A Base for Military-Civil Fusion in the Cyber Domain", CSET Issue Brief (July 2021), https://cset.georgetown.edu/wp-content/uploads/CSET-Chinas-National-Cybersecurity-Center.pdf, pp. 1–2, 9–38, accessed September 5 2024.

122 Peter Mattis, "Beyond Spy vs. Spy: The Analytic Challenge of Understanding Chinese Intelligence Services", *Studies in Intelligence*, Vol. 56, No. 3 (September 2012), pp. 53–54.

123 This book aligns with, and builds on, earlier work. See for example Didi Kirsten Tatlow, Greg Walton, and Anna B. Puglisi, "The Impact of China's Policies", in Hannas and Tatlow (eds.), *China's Quest for Foreign Technology*, pp. 205–222.

124 Mathew M. Aid, "Inside the NSA's Ultra-secret China Hacking Group: Deep within the National Security Agency, an Elite, Rarely Discussed Team of Hackers and Spies is Targeting America's Enemies Abroad" (June 10 2013), https://foreignpolicy.com/2013/06/10/inside-the-nsas-ultra-secret-china-hacking-group/, accessed June 28 2019.

gain access to hard targets) and later compromise of the CIA's covert communications system.[125]

What Western intelligence seeks from China is in traditional areas of politico-military secrets and decisionmaking.[126] For this and other reasons Chinese counterintelligence continues to be highly active, further making China a hard target. Remotely recruiting useful and reliable assets in places like China is no easy task unless they decide to "walk in" and offer their services. As well as their own counterintelligence activities, the PRC also continues to engage in traditional spycraft. It is a multi-pronged, multi-layered approach and a whole-of-nation effort where businesses, universities, and individuals are leveraged as part of Civil–Military Integration/Fusion (CMI/CMF).[127] This includes HUMINT gathering and exploitation by leveraging the "MICE" framework (Money, Ideology, Compromise/Coercion, and Ego).[128]

Su Bin, a spotter in the aviation industry for the PRC, was one such case. Another, in late 2024, involved Britain's Prince Andrew.[129] Honey traps are also common. This includes Fang Fang (aka Christine Fang), a modern-day Mata Hari who tried to seduce local U.S. politicians and congressmen.[130] Chinese intelligence also

125 Mark Mazzetti, Adam Goldman, Michael S. Schmidt, and Matt Apuzzo, "Killing C.I.A. Informants, China Crippled U.S. Spying Operations" (May 20 2017), https://www.nytimes.com/2017/05/20/world/asia/china-cia-spies-espionage.html, accessed June 27 2019. https://intelnews.org/tag/nsa-office-of-tailored-access-operations/, accessed January 23 2020.

126 Inkster, "The Chinese Intelligence Agencies", in Lindsay et al., *China and Cybersecurity*, p. 47.

127 Christopher Wray, Director Federal Bureau of Investigation, Hudson Institute Video Event: China's Attempt to Influence U.S. Institutions, Washington, D.C., "The Threat Posed by the Chinese Government and the Chinese Communist Party to the Economic and National Security of the United States" (July 7 2020), https://www.fbi.gov/news/speeches/the-threat-posed-by-the-chinese-government-and-the-chinese-communist-party-to-the-economic-and-national-security-of-the-united-states, accessed November 5 2021.

128 Aruna Viswanatha and Dustin Volz, "China's Spying Poses Rising Threat to U.S." (April 28 2019), https://www.wsj.com/articles/chinas-spying-poses-rising-threat-to-u-s-11556359201, Gordon Corera, "Looking for China's Spies" (December 19 2018), https://www.bbc.co.uk/news/resources/idt-sh/Looking_for_Chinas_spies. Both accessed May 9 2019.

129 Dominic Casciani and Sean Coughlan, "Alleged Chinese Spy had 'Unusual Degree of Trust' with Andrew" (December 13 2024), https://www.bbc.co.uk/news/articles/cd75vwdg3yvo, accessed December 13 2024.

130 Mark Moore, "Suspected Chinese Spy Reportedly Slept With, Courted US Officials to Gain Intel" (December 8 2020), https://nypost.com/2020/12/08/suspected-chinese-spy-slept-with-courted-us-politicians-report/, accessed November 5 2021. Bethany Allen-Ebrahimian and Zach Dorfman, "Exclusive: Suspected Chinese Spy Targeted California Politicians" (December 8 2020), https://www.axios.com/2020/12/08/china-spy-california-politicians, accessed November 10 2024.

actively recruits agents from rival Foreign Intelligence Services.[131] Some have Chinese heritage. These include former CIA officer Jerry Chun Shing Lee and CIA officer Alexander Yuk Ching Ma. Non-Chinese include former CIA case officer Kevin Mallory, U.S. State Department employee Candace Claiborne, and Ron Rockwell Hansen, who worked for the Defense Intelligence Agency. Chinese intelligence also recruits academics. Among them: Zhengdong Cheng, Gang Chen, and Mingqing Xiao. These and other cases were outlined in chapter 3.

In Autmn 2024, a deep-cover intelligence agent was arrested on suspicion of supplying intelligence on the transportation of defense equipment from a German arms manufacturer. This was passed to her handler, who had already been detained whilst working for the office of Maximilian Krah, a member of the European Parliament representing the right-wing nationalist party, Alternative for Deutschland. He had allegedly been passing intelligence from within the European Parliament.[132] Across the world, politicians, government employees, large defense contractors, commercial sector companies, and those in the supply chain have been targeted over long periods of time. This has included Chinese moles discovered within the FBI.[133]

The cases of AMSC, Sinovel, Trelleborg Offshore, and Taizhou CBMF (also in chapter 3) evidence how pervasive these efforts are. Chinese efforts are allied to hacked personal data. This assists in identifying key individuals and helping decide who might be vulnerable or susceptible to inducement. OSINT and hacked personal data together help China potentially recruit individuals or contacts not previously thought to be susceptible to approaches. This is why the 2013–2015 OPM breach (chapter 2) was very important. Whether cyberespionage should be considered a form of covert action (comparable to Russian active measures) has also been the

131 Arturo G. Munoz, "Intelligence in Public Media", *Studies in Intelligence*, Vol. 59, No. 4 (Extracts, December 2015), p. 33, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol-59-no-4/pdfs/Munoz-Chinese-Industrial-Espionage.pdf, accessed November 9 2016.

132 Csongor Körömi, "Germany Arrests Woman for Passing Defense Info to China via EU Lawmaker's Aide" (October 1 2024), https://www.politico.eu/article/chinese-spy-working-far-right-mep-aide-arrested-germany-secret-service-maximilian-krah/. Caroline Wheeler, Harry Yorke, Dipesh Gadher, and Tim Shipman, "Commons Worker Arrested after Allegedly Spying for China: British Parliamentary Researcher had Links to MPs with Classified Information" (September 10 2023), https://www.thetimes.co.uk/article/british-national-arrested-suspicion-china-spy-parliamentary-researcher-xrtbrw86m. Both accessed October 3 2024.

133 Former FBI Employee Sentenced in Manhattan Federal Court to 24 Months in Prison for Acting as an Agent of China (January 20 2017), https://www.justice.gov/usao-sdny/pr/former-fbi-employee-sentenced-manhattan-federal-court-24-months-prison-acting-agent, accessed March 18 2024.

subject of study.[134] One of the main themes in this book, and in *Cyberwarfare: Threats to Critical Infrastructure*, is that cyberespionage has characteristics that create threatening ambiguity between intelligence gathering and offensive operations.[135]

7 The Chinese Dream

China's 2015 Military Strategy stated:

> China's national strategic goal is to complete the building of a moderately prosperous society in all respects by 2021 when the CPC celebrates its centenary; and the building of a modern socialist country that is prosperous, strong, democratic, culturally advanced and harmonious by 2049 when the People's Republic of China (PRC) marks its centenary. It is a Chinese Dream of achieving the great rejuvenation of the Chinese nation. The Chinese Dream is to make the country strong. China's armed forces take their dream of making the military strong as part of the Chinese Dream. Without a strong military, a country can be neither safe nor strong. In the new historical period, aiming at the CPC's goal of building a strong military in the new situation, China's armed forces will unswervingly adhere to the principle of the CPC's absolute leadership, uphold combat effectiveness as the sole and fundamental standard, carry on their glorious traditions, and work to build themselves into a people's military that follows the CPC's commands, can fight and win, and … the armed forces will continue to follow the path of civil-military integration (CMI), actively participate in the country's economic and social construction, and firmly maintain social stability, so as to remain a staunch force for upholding the CPC's ruling position and a reliable force for developing socialism with Chinese characteristics.[136]

There is no doubt that cyberespionage allied to traditional spycraft from the West and in other parts of the world has aided China's long-term development and shortened its pathways to development. This includes in the military realm, and China has long aimed to learn from the West through its universities, businesses, and culture. Company acquisitions and mergers have also aided their development and indirect civilian technology transfer can shrink research or development times whilst also producing direct socio-economic benefits.

---

134 Michael Warner, "A Matter of Trust: Covert Action Reconsidered", *Studies in Intelligence*, Vol. 63, No. 4 (December 2019), pp. 33–41.

135 Stoddart, *Cyberwarfare*, pp. 1–51, 401–429.

136 "Full text: China's Military Strategy (Xinhua)" (May 26 2015).

Still, replicating, reverse engineering, or refining technologies are not always beneficial and can stifle innovation.[137] The practices which China has adopted can shorten pathways to development both for China and in the nations, regions, and sectors China is investing in through the BRI. The BRI, Made in China 2025, and CMI/CMF are described as three tributaries of Chinese geostrategic policy.[138] Made in China 2025 aims to produce more indigenous products, which may lead to a decrease in Chinese cyberespionage. However, the targets and scale and their ongoing espionage campaigns lead to the conclusion they are still learning to innovate. To this and other ends China can conduct cyberespionage on a scale that no other nation can currently match (whilst bearing in mind that current and future AI and quantum-computing capabilities might alter that calculation).

This includes utilizing 'lone wolves" and patriotic sub-state collectives.[139] Through one group alone, "Red Hacker Alliance", as many as 300,000 hackers might be able to be called upon as proxies or privateers.[140] Whilst there was no evidence of direct PLA involvement in the Red Hacker Alliance, there was ideological overlap between this group and the CCP/PLA. Not only can these "netizen" groups provide plausible deniability, but their activities can also benefit the state (partly because of sheer numbers and the vast volume of information/intelligence they can gather).[141] Similar Chinese actors have included "KeyBoy", "Honker Union", and the "Network Crack Program Hacker Group".[142]

---

137 Jon R. Lindsay and Tai Ming Cheung, "From Exploitation to Innovation Acquisition, Absorption, and Application", in Lindsay et al., *China and Cybersecurity*, pp. 51–86.

138 Thomas, *The Chinese Way of War: How Has it Changed?*, p. 22.

139 Wortzel, *The Chinese People's Liberation Army and Information Warfare*, p. 23.

140 Nigel Inkster, "China's Cyber Power", *Adelphi*, Vol. 55, Issue 456 (2015), p. 68. Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (Cambridge: Cambridge University Press, 2018), pp. 107–119.

141 Tobias Feakin, "Enter the Cyber Dragon: Understanding Chinese Intelligence Agencies' Cyber Capabilities", Australian Strategic Policy Institute Special Report, Issue 50 (June 2013), p. 4, https://www.aspi.org.au/report/special-report-enter-cyber-dragon-understanding-chinese-intelligence-agencies-cyber, accessed January 23 2020.

142 Feakin, "Enter the Cyber Dragon", p. 4. Bart Parys, "The KeyBoys are Back in Town" (November 2 2017), https://www.pwc.co.uk/issues/cyber-security-data-privacy/research/the-keyboys-are-back-in-town.html. Wun Nan, "From Hackers to Entrepreneurs: The Sino-US Cyberwar Veterans Going Straight" (August 21 2013), https://www.scmp.com/news/china/article/1298200/hackers-entrepreneurs-sino-us-cyberwar-veterans-going-straight. Ken Dunham and Jim Melnick, "'Wicked Rose' and the NCPH Hacking Group", https://krebsonsecurity.com/wp-content/uploads/2012/11/WickedRose_andNCPH.pdf. All accessed January 9 2020.

Through to 2009 these "patriotic hackers" were more of a nuisance than a strategic threat including in hot spots like Taiwan.[143] Following the formation of the PLA's Strategic Support Force in 2015, China's cyber operations and campaigns became more centrally controlled and directed.[144] In 2017, legislation (most notably a National Intelligence Law) sought to draw cybercriminal groups and lone wolves into state service as privateers.[145] This included foreign intelligence collection for the MSS.[146] The second series of major reorganizations begun in 2024 might point to further top-down coordination. Industrial and corporate espionage by Chinese companies and individuals like Su Bin have also aided China's hacking of civilian and military targets. Su Bin will not have been the only "target spotter" utilized by China.

Larry Wortzel testified in 2013, "There is an urgent need for Washington to compel Beijing to change its approach to cyberspace and deter future Chinese cyber theft. The Chinese government does not appear to be inclined to curb its cyber espionage in any substantial way. Merely naming will not affect this centrally directed behavior."[147] Washington is not the only capital affected. This is of wide concern across Europe and the Asia-Pacific, and includes a wider spectrum of activities beyond intellectual property theft. This includes mis- and disinformation and soft-power campaigns of coercion and propaganda. At the far end of the spectrum is the potential for cyberwar.[148]

---

143 James Mulvenon, "PLA Computer Network Operations: Scenarios Doctrine, Organizations, and Capability", in Roy Kamphausen, David Lai, and Andrew Scobell (eds.), *Beyond the Strait: PLA Missions Other Than Taiwan* (Carlisle, PA: NBR, 2009), pp. 255–257, 277–280.

144 FireEye iSight Intelligence, "Redline Drawn: China Recalculates its Use of Cyber Espionage" (June 2016), p. 15, https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-china-espionage.pdf, accessed February 3 2019.

145 Murray Scot Tanner, "Beijing's New National Intelligence Law: From Defense to Offense" (July 20 2017), https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense, accessed March 11 2020.

146 Nigel Inkster, "China's Draft Intelligence Law" (May 26 2017), https://www.iiss.org/blogs/analysis/2017/05/china-draft-intelligence-law, accessed March 11 2020.

147 '"Cyber Espionage and the Theft of U.S. Intellectual Property and Technology', Testimony of Larry M. Wortzel before the House of Representatives Committee on Energy and Commerce Subcommittee on Oversight and Investigations July 9, 2013 Summary of Testimony", https://docs.house.gov/meetings/IF/IF02/20130709/101104/HHRG-113-IF02-Wstate-WortzelL-20130709-U1.pdf, accessed April 7 2019.

148 Sascha Dominik (Dov) Bachmann, Andrew Dowse, and Håkan Gunneriusson, "Competition Short of War – How Russia's Hybrid and Grey-Zone Warfare are a Blueprint for China's Global Power Ambitions", *Australian Journal of Defence and Strategic Studies*, Vol. 1, No.1 (January 2019), p. 54.

As chapter 1 detailed, these sets of issues have been under study since the early 1990s. How these theorems and stratagems were operationalized was the subject of chapter 2. Among a long list of campaigns going back to the early 1990s, the potential for pivoting from cyberespionage to destructive cyberwar was particularly apparent in the 2021 "Volt Typhoon" campaign.[149] Whilst the CCP–PLA is aiming to further remedy its internal challenges, "success in war will remain uncertain. Ultimately, victory on the battlefield depends on where the battle is fought and against whom."[150] With this in mind, China has also engaged in military-to-military cooperation with Russia.

8 Sino-Russian dialogues: military-politico cooperation, intelligence sharing, and agreements

The PRC and Russia have been in increasing bilateral dialogues since around 2009. For a time this was centered on the annual International Forum for Information Security (usually held in Garmisch-Partenkirchen in Germany).[151] From the mid-2000s the organizer of this forum was Moscow State University's Institute for Information Security Issues. This may have played an important role in creating policy recommendations at the highest level. It also facilitated bilateral "track 2" meetings between European and Asian officials and experts. This included discussions on cyberspace, the Internet, and information security issues.[152]

It is suggested that deterrence to hostile Information Warfare was discussed through Sino-Russian dialogues in 2010 and 2011. This included discussions on legal frameworks around "information behavior", international information security, attributing cyberattacks, and content monitoring and filtering.[153] Sino-Russian meetings are also held as part of the Valdai Group, established in 2004 to examine a range of international issues, with a stated aim through to 2014 of "telling the world about Russia".[154] This is one of a number of fora for bilateral and multilateral meetings.

---

149 "Statement of Michael S. Rogers, Commander United States Cyber Command, before the Senate Committee on Armed Services 9 May 2017", https://www.armed-services.senate.gov/imo/media/doc/Rogers_05-09-17.pdf, accessed March 16 2024.

150 Noon and Bassler, "Schrodinger's Military?".

151 Thomas, *Three Faces of the Cyber Dragon*, p. 29. Julien Nocetti, "Contest and Conquest: Russia and Global Internet Governance", *International Affairs*, Vol. 91, Issue 1 (January 2015), pp. 111–130.

152 Nocetti, "Contest and Conquest", p. 119.

153 Thomas, *Three Faces of the Cyber Dragon*, p. 149.

154 "Valdai Discussion Club", https://valdaiclub.com/, accessed October 31 2021.

As part of this diplomatic rapprochement, China and Russia began to champion an International Code of Conduct for Information Security debated through the SCO.[155] This has been interpreted as a deliberate attempt to counterbalance U.S. hegemony on issues related to the Internet.[156] Western views were that this represented a Trojan horse for content control and Internet monitoring.[157] There are wider and strategically important issues at stake. Of 10 topics presented to the Russians in 2011, escalation models and (critical) civilian infrastructure were the top two. Industrial espionage was bottom of the list for Russia, where in China it was at the top.[158]

In April 2015 a Sino-Russian non-aggression cybersecurity agreement was signed. Its basic tenet was to facilitate the "further deepening of trust and development of cooperation … in the field of information and communication technologies".[159] This agreement has largely slipped off the radar but Article 3 dealing with bilateral cooperation is worthy of attention. Its subsections detail the:

> 2) establishment of channels of communication and contacts with a view to jointly respond to threats …
>
> 3) cooperation in the development and promotion of international law …
>
> 5) the exchange of information and cooperation in law enforcement to investigate cases involving the use of information and communication technologies for terrorist and criminal purposes …
>
> 7) cooperation … to ensure the safety of the critical information infrastructure …
>
> 8) the exchange of information on … [domestic] legislation
>
> 9) to contribute to improving the international legal framework and practical mechanisms of cooperation of the Parties …
>
> 11) to enhance cooperation and coordination among States Parties on issues of international information security within the framework of international organizations and fora (including the United Nations, the International Telecommunication Union, the International Organization for Standardization, the Shanghai Cooperation Organization, the BRICS countries [and] the Regional Forum of the Association of South-East Asian [Nations].

---

155 On the SCO see Piotr Dutkiewicz, Richard Sakwa, and Fyodor Lukyanov with Richard Burchill and Timofei Bordachev (eds.), *Eurasia on the Edge: Managing Complexity* (London: Rowman & Littlefield, 2018).

156 Hannes Ebert and Tim Maurer, "Contested Cyberspace and Rising Powers", *Third World Quarterly*, Vol. 34, No. 6 (July 2013), p. 1055.

157 Ebert and Maurer, "Contested Cyberspace and Rising Powers", p. 1055.

158 Thomas, *Three Faces of the Cyber Dragon*, pp. 149–150.

159 The agreement can be found in James A. Lewis, "Sino-Russian Cybersecurity Agreement 2015" (May 11 2015), https://www.csis.org/blogs/strategic-technologies-blog/sino-russian-cybersecurity-agreement-2015, accessed March 20 2019.

> 12) the promotion of research in the field of international information security, joint research work.
>
> 13) joint training of specialists, exchange of students and teachers from specialized higher education institutions;
>
> 14) conduct of meetings, conferences, seminars and other forums ...
>
> 15) the establishment of a mechanism for cooperation ... for the exchange of information and sharing of information on existing and potential risks, threats and vulnerabilities ...

Under Article 5 they were also aiming to "hold consultations on a regular basis" by "authorized representatives" twice yearly, "alternately in the Russian Federation and the People's Republic of China".[160] According to STRATFOR's 2018 analysis, Sino-Russian cyber cooperation includes opposition to the U.S./EU-led model of Internet/cyber governance and an open Internet, and its replacement with one founded on "cyber sovereignty". This includes "in-country data storage, facilitation of surveillance and much greater state control over online content and hardware".[161]

It has also been reported that the two countries have been sharing intelligence. In the early 2010s, the CIA's covert communications system is alleged to have been compromised by the Chinese government. Not only was this used to arrest or execute Chinese nationals spying for America but it was also used to identify Russians working for the CIA.[162] There is also an uncorroborated UK government-sourced report which appeared in *The Times* in June 2015 alleging that China and Russia had decrypted the unreleased files that Edward Snowden had exfiltrated from the NSA.[163] It has been suggested that around 200,000 documents were provided to journalists by Snowden before he fled Hong Kong whilst 1.3 million encrypted documents could have been retained.[164]

---

160 https://cyber-peace.org/wp-content/uploads/2013/05/RUS-CHN_CyberSecurityAgreement201504_InofficialTranslation.pdf, accessed March 20 2019. On Chinese views of law (including international law) see Cheng, *Cyber Dragon*, pp. 203–206.

161 "Joint Interests Against the U.S. Deepen the Sino-Russian Embrace" (November 5 2018), https://worldview.stratfor.com/article/china-russia-embrace-interests-us-deepens, accessed March 20 2019.

162 Mazzetti, Goldman, Schmidt, and Apuzzo, "Killing C.I.A. Informants".

163 Tom Harper, Richard Kerbaj, and Tim Shipman, "British Spies Betrayed to Russians and Chinese" (June 14 2015), https://www.thetimes.co.uk/article/british-spies-betrayed-to-russians-and-chinese-xxj7zx5n83d, accessed June 28 2019.

164 Michael B. Kelley, "Snowden May Have Some Clarifying to do after Bombshell Reports that Russia and China Accessed NSA Files" (June 13 2015), https://www.businessinsider.com/snowden-russia-china-and-nsa-files-2015-6?r=US&IR=T. Glenn Greenwald, the journalist responsible for breaking the story, claims this might be as few as 9–10,000 documents. Deb Riechmann, "Costs

China's 2015 military strategy noted, "China's armed forces will further their exchanges and cooperation with the Russian military within the framework of the comprehensive strategic partnership of coordination between China and Russia, and foster a comprehensive, diverse and sustainable framework to promote military relations in more fields and at more levels".[165] Sino-Russian dialogues had already led to technology transfers from Russia to China, especially Soviet-era aircraft sold under export licenses (aircraft and engines that China has historically struggled to reliably mass manufacture). This was gradually extended from 2012–2022 and included S-400 air defense systems, Mi-171 helicopters, submarine technology, and aircraft engines. This is also believed to extend into AI and space technologies.[166] Despite sales of advanced aircraft, engines, and air defense systems, "China has repeatedly stolen Russian technology and know-how, creating friction between Beijing and Moscow".[167]

Despite this friction, Russia and China have also conducted joint naval exercises since 2012.[168] This included Vostok-2018.[169] In total there were around 78 joint military exercises between 2003 and mid-2022 – over half of them since 2016. Further exercises have included the September 2024 "Ocean-24" naval exercise across the Pacific and Arctic Oceans, Mediterranean, Caspian Sea, and Baltic Sea, involving over 400 military vessels, 120 aircraft, and 90,000 personnel. This was the largest war game of its kind in 30 years.[170] According to the Center for Strategic and International Studies' ChinaPower project, there have been over 100 joint military exercises through to mid-2024.[171] At the same time, there is a "growing power disparity between the two countries, as China solidifies its position as the more 'se-

of Snowden Leak Still Mounting 5 Years Later" (June 4 2018), https://apnews.com/797f390ee28b4bfbb0e1b13cfedf0593. Both accessed June 28 2019.

165 "Full text: China's Military Strategy (Xinhua)" (May 26 2015).

166 Paul N. Schwartz, "The Changing Nature and Implications of Russian Military Transfers to China" (June 21 2021), https://www.csis.org/analysis/changing-nature-and-implications-russian-military-transfers-china, accessed September 14 2024.

167 Brian Hart, Bonny Lin, Matthew P. Funaiole, Samantha Lu, Hannah Price, Nicholas Kaufman, and Gavril Torrijos, "How Deep Are China–Russia Military Ties?", https://chinapower.csis.org/china-russia-military-cooperation-arms-sales-exercises/, accessed May 30 2023.

168 Described in chapter 4.

169 Dave Johnson, "VOSTOK 2018: Ten Years of Russian Strategic Exercises and Warfare Preparation" (December 20 2018), https://www.nato.int/docu/review/articles/2018/12/20/vostok-2018-ten-years-of-russian-strategic-exercises-and-warfare-preparation/index.html, accessed October 31 2021.

170 Anonymous, "Russia Begins Massive Naval Drills Together with China" (September 10 2024), https://apnews.com/article/russia-naval-air-drills-china-f941584643d6503df2b42dae7abe7f15, accessed September 14 2024.

171 "China–Russia Joint Military Exercises" (regularly updated), https://chinapower.csis.org/data/china-russia-joint-military-exercises/, accessed September 14 2024.

nior' partner". All the while, Russia's GDP has fallen to under $2 trillion, whilst China's is expected to surpass $30 trillion during the latter half of the 2020s.[172]

When Russia faced economic and diplomatic sanctions after the annexation of Crimea in 2014, exports and contacts became more valuable to Russia than China, including Russian oil and gas exports. Furthermore, as China's defense-industrial base has advanced, it has increasingly become less reliant on Russia to supply what the PLA needs. In addition, China has leached sensitive technologies from Russia through espionage and cyberespionage in at least 500 instances from 2004 onwards. This is all taking place against Russian concerns about arming a future rival/adversary.[173]

In terms of strategy, Russia has not only reached back to Soviet times, but also appears to have utilized Chinese ideas of Unrestricted Warfare and particularly Strategic Psychological War which China saw as a potential domestic threat after the Arab Spring began in 2011. That year Ye Zheng and Zhao Baoxian of the PLA's Academy of Military Sciences noted the importance of influence operations:

> Network psychological warfare is a mental and psychological game that unfolds in cyberspace. It has been referred to as "the politics of the heart". It is the extension and development of traditional psychological warfare in cyberspace … [and] the targets of network psychological operations have already expanded from the military to society and the people to achieve the "butterfly effect" and directly achieve political goals.[174]

Whilst distinct from Russia's multifaceted "Gerasimov doctrine"/strategy of "hybrid warfare", Chinese stratagems share similarities and vice versa. Chinese intelligence will also have taken note of Russian successes in its mis- and disinformation campaigns. This "holds that an adversary's political, social and economic institutions – particularly the media – should be targeted before a shooting war ever begins" combined with systematic "soft power" policies of "economic, social,

172 "Series: China–Russia Relations", https://chinapower.csis.org/series-china-russia-relations/, accessed May 30 2023.

173 Schwartz, "The Changing Nature". Erica Downs and Tatiana Mitrova, "How Much Energy Did China Import to Russia in 2022 Compared to 2021?", https://www.energypolicy.columbia.edu/qa-china-russia-energy-relations-one-year-after-the-invasion-of-ukraine/, accessed September 14 2024.

174 Ye Zheng and Zhao Baoxian, "How Do You Fight a Network War?", *Zhongguo Qingnian Bao Online*, June 3 2011. Quoted in Timothy Thomas, "Creating Cyber Strategists: Escaping the 'DIME' Mnemonic", *Defence Studies*, Vol. 14, No. 4 (2014), p. 376.

cultural and media initiatives".[175] Like Russia, China also uses proxies or privateers as cover for state-run or state-approved activities.[176]

They have also taken note of the effectiveness of Russian mainstream media propaganda, including outlets like RT (formerly Russia Today), on both foreign and domestic audiences.[177] Viewed in the light of how an aggressor nation can affect the views of a target state, Chinese theories of SPW look to have been directly incorporated into Russia's playbook after, or as part of, the "Gerasimov doctrine" of 2013.[178] This culminated in Russian election interference in the 2016 U.S. presidential election and the UK's Brexit vote. Whilst there might be Soviet-era/KGB antecedents, Russia, more than China, has also benefitted from the "Three Warfares". Russia has operationalized these concepts in highly effective campaigns.[179] The extent to which (or whether) this is the result of Chinese influences is currently unevidenced. However, thinking about the extent to which Chinese theorems might have influenced Kremlin decisionmaking is not unwarranted.

In the decade since Xi assumed office in 2013 through to March 2023, "within different bilateral and multilateral frameworks", Presidents Xi and Putin met around 40 times.[180] There are also frequent visits between Chinese and Russian officials, up to and including their Chiefs of Staff, with a direct hotline between their leaderships. Xi's first visit with Putin took place in Russia in March 2013.

---

175 Kent Harrington, "How Russian Cyber-meddling Can Inspire China", (February 6 2018), https://www.scmp.com/comment/opinion/article/2132222/how-russian-cyber-meddling-can-inspire-china, accessed October 31 2021.

176 Maurer, *Cyber Mercenaries*, pp. 107–119.

177 Elizabeth Chen, "China Learning From Russia's 'Emerging Great Power' Global Media Tactics", *China Brief*, Vol. 21, Issue 7 (April 12 2021), https://jamestown.org/program/china-learning-from-russias-emerging-great-power-global-media-tactics/, accessed August 31 2024.

178 Victor R. Morris, "Grading Gerasimov: Evaluating Russian Nonlinear War Through Modern Chinese Doctrine" (undated), https://smallwarsjournal.com/jrnl/art/grading-gerasimov-evaluating-russian-nonlinear-war-through-modern-chinese-doctrine. On Gerasimov see Mark Galeotti, "Putin's Hydra: Inside Russia's Intelligence Services", https://www.ecfr.eu/page/-/ECFR_169_-_PUTINS_HYDRA_INSIDE_THE_RUSSIAN_INTELLIGENCE_SERVICES_1513.pdf. Mark Galeotti, "(Mis)Understanding Russia's Two 'Hybrid Wars'", *Critique & Humanism*, Vol. 59, No. 1 (2018), p. 2. Reprinted in https://www.eurozine.com/misunderstanding-russias-two-hybrid-wars/?pdf. All accessed January 3 2018.

179 "Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security: A Minority Staff Report", Committee on Foreign Relations United States Senate (January 10 2018), pp. 1, 38, 65–140, 171–179, https://www.foreign.senate.gov/imo/media/doc/FinalRR.pdf, accessed November 5 2019.

180 Lily McElwee, Maria Snegovaya, Alexandra Chopenko, and Tina Dolbaia, "Xi Goes to Moscow: A Marriage of Inconvenience?" (March 28 2023), https://www.csis.org/analysis/xi-goes-moscow-marriage-inconvenience, accessed May 30 2023.

Prior to the Covid-19 pandemic they had last met in person at St. Petersburg in June 2019.[181] Over 30 intergovernmental and commercial deals were signed during this three-day visit which vowed "to improve bilateral ties amid US hostility".[182] They met again in June 2021 via video link, when they discussed a bilateral nuclear energy project. Putin and Xi are reported to stay in regular contact.

A spokesperson for the Chinese Foreign Ministry claimed, "It is fair to say that the China-Russia comprehensive strategic partnership of coordination for the new era is all-dimensional and all-weather. The sky is the limit for down-to-earth China–Russia cooperation, and we are full of confidence in the development of bilateral relations."[183] Further visits followed in February 2022 at the opening of the Winter Olympics in Shanghai, and September 2022 at a summit of the SCO, as well as in March 2023 in Moscow.[184] They also met at the third Belt and Road forum that October, [185] and again, along with their senior defense and security officials, in Beijing on May 16 2024. This was Putin's first overseas state visit since winning his fifth presidential election.[186] They were also pictured together alongside Indian Prime Minister Narendra Modi at the BRICS summit in October 2024.[187]

Former Secretary of Defense James Mattis' assertion that "I see little in the long term that aligns Russia and China" may echo "the Western conventional wisdom" but is, according to Alexander Gabuev of Moscow's Carnegie Foundation,

181 Jun Mai, "Can Friendship Between Xi Jinping and Vladimir Putin Really be Pillar of China–Russia Relations?" (June 7 2019), https://www.scmp.com/news/china/diplomacy/article/3013612/can-friendship-between-xi-jinping-and-vladimir-putin-really-be, accessed June 27 2019.

182 Viewed in person and "Chinese President Xi Jinping Meets Vladimir Putin on a Three-Day State Visit to Russia" (June 6 2019), https://www.youtube.com/watch?v=tF6vzSWBX0o, accessed June 27 2019.

183 Chen Qingqing and Cui Fandi, "Xi, Putin to Meet Online, Underscoring Unwavering Strategic Partnership" (June 27 2021), https://www.globaltimes.cn/page/202106/1227212.shtml, accessed October 17 2021.

184 McElwee, Snegovaya, Chopenko, and Dolbaia, "Xi Goes to Moscow".

185 Bonny Lin, Brian Hart, Samantha Lu, and Yu-Jie (Grace) Liao, "Analyzing the Latest Xi–Putin Meeting and China's Belt and Road Forum" (October 24 2023), https://chinapower.csis.org/analysis/xi-putin-meeting-belt-road-forum/, accessed September 14 2024.

186 Simone McCarthy, "China's Xi Jinping Rolls Out Red Carpet for Close Friend Putin in Strong Show of Unity" (May 16 2024), https://edition.cnn.com/2024/05/15/china/putin-xi-meeting-china-intl-hnk/index.html, accessed September 14 2024.

187 Vladimir Soldatkin and Guy Faulconbridge, "Putin Scores a BRICS Win with Rare Xi and Modi Show of Harmony" (October 23 2024), https://www.reuters.com/world/xi-modi-discuss-ukraine-war-with-putin-brics-considers-expansion-2024-10-23/, accessed November 10 2024.

"dangerously wrong".[188] Beijing and Moscow have moved closer after decades of disagreements including over border issues and Chinese cyberespionage, and both are separately evolving their own indigenous GPS-style satellite systems: China's Beidou and Russia's Glonass. Given their twentieth-century history of splits, competition, and sometime cooperation, "camps [are] developing around the question of whether the partnership is a genuine realignment or simply a marriage of convenience".[189] Future Sino-Russian cooperation is difficult to forecast but its evolution thus far is a cause of concern for many in the West.[190] Xi and his administration have also positioned themselves as honest brokers for a peace deal between Russia and Ukraine.[191]

9 Great power rivalry and gray areas

Whether offensively or defensively, cyber (in various forms and functions) and technology can be both a force multiplier and a force inhibitor, depending on its employment and the actors and agency involved. This conundrum brings into question "the desirability and the relevance of traditional military superiority" against the backcloth of "internal disintegration of fractured political systems".[192] For the Western world, and to varying degrees globally, the United States has possessed hegemonic military advantages (excluding nuclear weapons). This has helped build an established Western-led international order and help set a series of fundamental conditions pertaining to national security (especially evident through NATO). These fundamental conditions are under direct and indirect challenge, if not outright and long-term threat.

188 Alexander Gabuev, "Why Russia and China Are Strengthening Security Ties" (September 24 2018), https://carnegie.ru/2018/09/24/why-russia-and-china-are-strengthening-security-ties-pub-77333, accessed March 20 2019.

189 Eric Jacobson, "Sino-Russian Convergence in the Military Domain", *New Perspectives in Foreign Policy*, Issue 15 (Spring 2018), p. 3.

190 This is well captured in Oriana Skylar Mastro, "Sino-Russian Military Alignment and Its Implications for Global Security", *Security Studies*, Vol. 33, No. 2 (2024), pp. 254–290. See also Mallick, *China in the Cyber Domain*, pp. 305–306.

191 McElwee, Snegovaya, Chopenko, and Dolbaia, "Xi Goes to Moscow.

192 John Steinbruner, "Problems of Predominance: Implications of the U.S. Military Advantage" (September 1 1996), https://www.brookings.edu/articles/problems-of-predominance-implications-of-the-u-s-military-advantage/, accessed December 20 2018.

This means prevailing attitudes need to be critically reconsidered.[193] These relative politico-military advantages, a legacy of World War II and the Cold War, might be sustainable but the current posture might also outweigh the benefits. This particularly applies to large-scale military confrontations and military configurations in a cybered environment. China in particular is one of several states "maneuvering to fend off intimidation in a manner that can be generally dangerous".[194] Moreover, there are no indications that the CCP–PLA believes war or armed conflict is inevitable.[195] Nevertheless, in 2018 a bipartisan U.S. Congressional commission appointed to examine the 2018 National Defense Strategy arrived at a pessimistic assessment they described as a "crisis". The commission concluded that:

> America's two most powerful competitors – China and Russia – have developed national strategies for enhancing their influence and undermining key U.S. interests that extend far beyond military competition. Encompassing economic, diplomatic, covert, political, and other initiatives, those strategies draw on the full array of foreign policy tools; they include many actions that fall short of war but nonetheless alter the status quo in dangerous ways.[196]

This includes the employment of creative asymmetrical tactics which for China includes intimidation and coercion in the gray zone between peace and war.[197] Particularly since the open outbreak of the Ukraine War in February 2022 Russia has gone further still.

Crisis or not, political dysfunction, partisanship, and electoral volatility are not the only forces at work. In the United States as well as among the European members of NATO, military spending has flatlined or decreased since the end of the Cold War. This needed addressing. In February 2025, the British government announced that it was raising defense spending to 2.5% of GDP from April 2027, rising to 3% in the next parliament. This is Britain's largest reallocation to the defense budget (and increased investment) since the Cold War.[198] As the second

---

193 This formed part of the conclusion to the excellent 2015 edited book *China and Cybersecurity* led by Jon R. Lindsay. Jon R. Lindsay and Derek Reveron, "Conclusion: The Rise of China and the Future of Cybersecurity", in Lindsay et al., *China and Cybersecurity*, pp. 333–354.

194 Steinbruner, "Problems of Predominance".

195 Cheng, *Cyber Dragon*, pp. 202–205, 207–212.

196 "Providing for the Common Defense", pp. vi and 63.

197 "Providing for the Common Defense", p. 5. For (sometimes) countervailing analysis see Cheng, *Cyber Dragon*, pp. 217–221.

198 Press Release: Prime Minister Sets Out Biggest Sustained Increase in Defence Spending since the Cold War, Protecting British People in New Era for National Security (February 25 2025), https://www.gov.uk/government/news/prime-minister-sets-out-biggest-sustained-increase-in-defence-

Trump administration has made waves regarding NATO Europe's decline in defense spending, NATO allies raised defense expenditure during 2024 after years of stagnation.[199] This is combined with prospects for further increases to fund material capabilities and potential peacekeeping missions against the background of the Russo-Ukraine War. Following the addition of Finland and Sweden to NATO's ranks in 2023 and 2024, increased "burden sharing" between the United States and NATO's European allies is intended to signal to the United States that Ukraine's future security and the security of NATO Europe are seen as intimately bound together.[200] These increases and future discussions are also intended to shore up American support for NATO should the U.S. once more "pivot to Asia" to address the growing challenges posed by China or return to a pre-World War II policy of increased isolationism.[201]

However, whether in terms of force size or service configurations, reconfigurations, or joint operations, "gray zone" aggression poses non-military threats as well military risks. These portend a much wider and deeper series of changes. Cyber, the fifth domain of warfare, is the most profound of those changes because it increasingly binds land, sea, air, and space capabilities into a functioning whole. Whilst it is not changing the fundamental character of war, it continues to change the conduct of war.

In addition, for the intelligence community a two-decade-long focus on terrorism and insurgency has led to a decreased focus on state-level threats and specialist Sinologists and Kremlinologists.[202] Neither of these threats has gone away. Instead, threats and threat actors have become more numerous and more serious than at any time since the end of the Cold War. Now, the U.S. military (and its NATO, and non-NATO, allies and friends):

---

spending-since-the-cold-war-protecting-british-people-in-new-era-for-national-security, accessed February 28 2025.

199 Press Release: Defence Expenditure of NATO Countries (2014–2024), https://www.nato.int/nato_static_fl2014/assets/pdf/2024/6/pdf/240617-def-exp-2024-en.pdf, accessed 28 February 2025.

200 Emma Ashford and Jennifer Kavanagh, "Europe Isn't Ready for Trump 2.0: Washington is Likely to Reduce its Troop Presence and Demand Even Higher Defense Spending" (January 23 2025), https://foreignpolicy.com/2025/01/23/trump-eu-nato-europe-defense-spending-troop-deployments-burden-sharing/, accessed February 28 2025.

201 Christopher McKnight Nichols, "The Enduring Power of Isolationism: An Historical Perspective", *Orbis*, Vol. 57, Issue 3 (Summer 2013), pp. 390–407.

202 Eric Schmitt, "U.S. Military's Global Edge has Diminished, Strategy Review Finds" (November 14 2018), https://www.nytimes.com/2018/11/14/us/politics/defense-strategy-china-russia-.html, accessed December 20 2018.

> must address the threats posed by major-power rivals, dangerous regional challengers, and terrorists simultaneously; it must deal with geopolitical conflict, gray-zone aggression, and instability from one end of Eurasia to the other. It must also prepare for the prospect that the U.S. military might be called into action in a country, region, or contingency that is not currently envisioned.[203]

Increases in defense expenditure and reorienting from a defense posture built on counterterrorism and counterinsurgency towards one which prioritizes preparations for a return to major power competition and conflict which supports and draws on America's network of alliances might not be enough.[204] It includes a more comprehensive understanding and appreciation of how and why China has emerged as a peer rival to the United States since the end of the Cold War and domestic and international developments since.

This entails fundamental assessments of past, current, and future vulnerabilities and the extent to which a clash of civilizations has become a more prevalent domestic issue as well as an increasing feature of international relations.[205] This also applies to how American, Western, and non-Western innovation has been mined and reforged with a clear-minded idea of the economic costs and benefits it has brought to the PRC. National security and the underlying strength of Western economies are currently being simultaneously undermined. Whether domestic political divides can be bridged by whole-of-government or whole-of-nation cooperation is not only an American issue. Diplomatic statecraft, other non-military tools, and the strengthening or weakening of the Western (and wider) system of alliances and shared interests will also play their part, because "Without such a holistic approach, the United States will be at a competitive disadvantage and will remain ill-equipped to preserve its security and its global interests amid intensifying challenges".[206]

This extends beyond the United States, but America is a hegemonic power in the West. Not only is it the world's leading economy, but it is also the lead innovator. This has also made it cyber dependent, and one of the elements undercutting the U.S. advantage is cyberespionage and China's (and Russia's) capabilities and capacity to hold critical infrastructure at risk. This includes risks to its military. This very much includes Chinese cyberespionage, including its existing capabilities and

---

203 "Providing for the Common Defense", p. 10.

204 "Providing for the Common Defense", p. vi.

205 Masud Chand, "Is there a Clash of Civilizations? Cultures and Institutions across Civilizations", *Global Business & Finance Review*, Vol. 27, Issue 3 (June 2022), pp. 75–97. Jeffrey Haynes (ed.), *A Quarter Century of the "Clash of Civilizations"* (Abingdon: Routledge, 2021).

206 "Providing for the Common Defense", p. 63.

capacity to engage in cyberwarfare or a range of cyber operations short of major disruption or destruction. This is a dynamic aspect of the security dilemma calculus.

As Colin S. Gray identified, "America is the land of technological marvels and of extraordinary technology dependency … American soldiers say that the human beings matter most, but in practice, the American way of war, past, present, and prospectively future, is quintessentially and uniquely technologically dependent".[207] The U.S. economy and its military owe much to innovation. Chinese cyber-espionage has used this as a shortcut to catch up and challenge U.S. power. How and whether the U.S. should "hack back" is a policy option, but for now, as with Russia, the chosen options have been economic sanctions and a "trade war" with a policy to "name and shame" Chinese hackers and those of other nations. Whether this is the best course of action or sustainable is questionable. Far more important still, whether now or in the future, one hopes that "Thucydides' Trap" will not be tested.[208]

Whatever readers perceive about the threat picture, this also needs to be carefully weighed alongside many positives. Trade benefits and increasing cultural understanding are among them. In addition, the PRC (led by the CCP) has become a pivotal international actor. Without engaging and understanding China, global politics will be worse off. This includes issues of global-level importance including questions around climate change, international security, and economic trade and development. In addition, there are people across the planet with Chinese roots stepping across generations. Through philosophy, military thought, art, buildings, literature, and religion what has been imparted is a rich and diverse cultural heritage that develops and influences through to the present. Following centuries of upheaval and foreign domination, China and its people have much to be proud of. We are wiser people by learning from successive Chinese administrations and developments.

207 Colin S. Gray, "The American Way of War", in Anthony D. McIvor (ed.), *Rethinking the Principles of War* (Annapolis, MD: Naval Institute Press, 2005), p. 29.

208 Whether we ever arrive at "Thucydides' Trap" through policy choices, calculation, miscalculation, deployments, or missteps by policymakers and policymaking is a scenario that is difficult to forecast. The actor–agency debate, strategic culture, and international relations perspectives including realism and neo-liberalism (and more besides) are helpful lenses.