Introduction

China is a rising power. By some indices it has surpassed the United States. Although the American economy remains the largest on earth (and has been since the 1870s), and the conventional forces of the United States military remain larger and more capable than any of its peers, including China, that advantage is under challenge.[1] There are many ways of looking at this challenge, but any perspective should have a mind to the big, long-term picture.[2] This is where this book primarily positions itself in demonstrating not only how cyberespionage is enabling China to become a material long-term challenge economically and militarily to the United States – and the West more widely – but also how cyberespionage enables a growing capacity to engage in cyberwarfare through attacks on critical infrastructure (CI).[3]

China, which has been cooperating with Russia on mutual security concerns since about 2009, is, to an even greater degree than Russia, able to hold Western CI at-risk through its cyberespionage campaigns whilst engaging in major and sustained intellectual property (IP) theft. This leads to U.S. research (and that of other nations) being reengineered, developed, and deployed by China. This includes China's military programs. Many sectors of the economy are examined throughout but the primary consideration of this book is concentrated upon how cyberespionage has been used to advance China's military, as well as how it has aided China's marked economic growth.

1 The PRC and People's Liberation Army

The People's Republic of China (PRC) has been ruled by the Chinese Communist Party (CCP[4]) since the end of the Chinese Civil War in 1949. The island of Taiwan,

1 "Military Expenditure", https://www.sipri.org/research/armament-and-disarmament/arms-and-military-expenditure/military-expenditure, accessed February 26 2024.

2 Paul Kennedy, *The Rise and Fall of the Great Powers: Economic Change and Military Conflict from 1500 to 2000* (New York: Random House, 1987). Christopher Coker, *The Improbable War: China, the United States and the Logic of Great Power Conflict* (London: Hurst & Co., 2015). Christopher Coker, *Future War* (Cambridge: Polity Press, 2015). Robert Farley, "Yes, the U.S. Military Is In Decline. And There Is No Need to Panic" (July 5 2018), https://nationalinterest.org/blog/buzz/yes-us-military-decline-and-there-no-need-panic-25057, accessed December 20 2018. The rise and decline of ideas of Network Centric Warfare which appeared after the 2003 Gulf War are part of this larger picture.

3 Kristan Stoddart, *Cyberwarfare: Threats to Critical Infrastructure* (London: Palgrave, 2022).

4 Also frequently abbreviated as the CPC (Communist Party of China).

https://doi.org/10.1515/9783111575513-003

where nationalist forces under Chiang Kai-shek retreated to form their own government, is seen by the CCP as China's 23rd province (and a source of dispute and tension ever since). China's population has more than doubled since 1960 and at the last census in 2022 stood at 1.4 billion people, the world's largest population.[5] This is matched only by its southwest neighbor, India (which overtook China during 2023). Unlike India, China's population is in decline and could fall below 1 billion before the end of the century.[6] China's population is also aging as life expectancy has increased, and in 2024 the People's Congress announced it would gradually raise the retirement age in order to try to combat the deep set of demographic-economic issues it faces.[7]

It is the third largest nation by area at around 9,600,000 km^2. China, historically and geographically the "Middle Kingdom", shares borders with 14 nations. Four of these (Russia, India, Pakistan, and North Korea) are fellow nuclear weapons states. Its major population centers are concentrated in and around 23 metropolitan cities in the east and south of the country. This has led to steady southeasterly migration from rural inland provinces to coastal cities for the financial and social opportunities provided. This massive influx of labor has helped fuel China's remarkable development. Inland, growing urban and suburban conurbations support and supply these coastal metropolises. Although China has unified, it is still a diverse nation with differing regional customs and local dialects as well as widely varying geography and topography with a long and rich history (including a history of colonization by foreign powers).[8]

The PRC has been headed by President Xi Jinping since 2012. Born in Beijing in 1953, Xi is a third-term president as well as General Secretary of the CCP and Chair-

5 The last Chinese census was in 2020.

6 This is due to falling birth rates and, like many other developed states, China has an aging population. India's population is predicted to grow for decades. "World Population Prospects 2022, Summary of Results", https://www.un.org/development/desa/pd/sites/www.un.org.development.desa.pd/files/wpp2022_summary_of_results.pdf, p. i. United Nations Department of Economic and Social Affairs, Policy Brief No. 153 (April 2023), https://www.un.org/development/desa/pd/sites/www.un.org.development.desa.pd/files/undesa_pd_2023_policy-brief-153.pdf. Both accessed February 21 2024.

7 Simone McCarthy, "For Decades, Chinese Workers Have Retired Relatively Early. That's About to Change" (September 13 2024), https://edition.cnn.com/2024/09/13/china/china-raises-retirement-age-intl-hnk/index.html, accessed September 14 2024.

8 Hai-Jun Huang, Tian Xia, Qiong Tian, Tian-Liang Liu, Chenlan Wang, and Daqing Li, "Transportation Issues in Developing China's Urban Agglomerations", *Transport Policy*, Vol. 85, Issue C (January 2020), pp. A1-A22. Wei Qi, Guy J. Abel, and Shenghe Liu, "Geographic Transformation of China's Internal Population Migration from 1995 to 2015: Insights from the Migration Centerline", *Applied Geography*, Vol. 135 (October 2021), 102564.

man of the Central Military Commission (CMC).[9] His third term broke an established norm to limit the consolidation of power in one individual. Critics suggest this is part of trends towards increasing personal authoritarianism and a break from post-1989 reform-era rules. The extent to which checks and balances on power at the top echelons of Chinese politics have been removed or reconstituted remains subject of debate. This is especially in the context of anti-corruption reforms and the removal of key officials from government or civilian office with little or no public explanation.[10] These include then Foreign Minister, Qin Gang, and Minister of Defense, Li Shangfu in 2023.[11]

The military arm of the PRC is the People's Liberation Army (PLA). Having been established in 1927, the PLA predates the founding of the PRC.[12] The PLA is now "organizationally part of the party apparatus" with "Career military officers for the most part ... party members".[13] The PLA is the world's largest standing army and China's defense budget is second only to the United States'. In 2019 it was an estimated ¥166 trillion (yuan) ($240 billion USD). The 2020 budget was estimated at $252 billion USD. By comparison, U.S. defense expenditure was estimated at $778 billion for 2020. Between 2011 and 2020 China's defense budget rose 76 percent. According to detailed analysis by the widely respected Stockholm International Peace Research Institute (SIPRI), China's spend on defense is the lengthiest sustained succession of continuous increases by any state in their Military Expenditure Database. To set this in a global context, the top five spenders in 2020 were the United States, China, India ($72.9 billion), Russia ($61.7 billion) and the United Kingdom ($59.2 billion). Between them, they accounted for 62 per-

9 "Xi Jinping 习近平", https://www.brookings.edu/wp-content/uploads/2018/03/china_20180318_xi_jinping_profile.pdf, accessed February 24 2024. On top-down internal party structure see Dean Cheng, *Cyber Dragon: Inside China's Information Warfare and Cyber Operations* (Santa Barbara, CA: Praeger, 2017), pp. 3–4.

10 Björn Alexander Düben, "Xi Jinping and the End of Chinese Exceptionalism", *Problems of Post-Communism*, Vol. 67, No. 2 (2020), pp. 111–128. Jenny Li, "China Under Xi Xinping", *Journal of International Affairs*, Vol. 75, No. 1 (Fall/Winter 2022), pp. 261–272. Jeffrey A. Bader, "7 Things You Need to Know about Lifting Term Limits for Xi Jinping" (February 27 2018), https://www.brookings.edu/articles/7-things-you-need-to-know-about-lifting-term-limits-for-xi-jinping/, accessed February 24 2024.

11 Susan V. Lawrence, Karen M. Sutter, "China Primer: U.S.–China Relations" (October 24 2023), https://crsreports.congress.gov/product/pdf/IF/IF10119, accessed November 8 2024.

12 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.

13 Defense Intelligence Agency, *China Military Power: Modernizing a Force to Fight and Win* (2019), p. 13, www.dia.mil/Military-Power-Publications, accessed April 9 2019.

cent of global military expenditure in the year prior to the two-year disruption caused by the 2020–2022 Covid-19 pandemic.

Meanwhile, Japan, to China's east, spent $49.1 billion, South Korea (separated by North Korea on its southern border) $45.7 billion, and Australia, to its southeast, $27.5 billion. Aside from China, they spent the most on defense in Asia-Oceania. For China, overall military spending as a share of Gross Domestic Product (GDP) rose despite the economic dislocation that resulted from Covid-19.[14] In 2022, China's defense expenditure represented 13 percent of the global total. The United States, at 39 percent, spent three times as much as China – its nearest rival.[15] Official Chinese government figures put expenditure for 2023 at ¥1.55 trillion (around $224.79 billion), a 7.2 percent increase on 2022. Official government sources indicate that China has been spending around 1.5 percent of its GDP on defense. The U.S., around 3.5 percent.[16] NATO members are committed to at least 2 percent. rising to between 3.5–5 percent by 2035. This new spending commitment followed NATO's Hague Summit in June 2025 and discussions with the second Trump administration centered on the longstanding issue of burden sharing.[17] In 2024 a further 7.2 percent increase was announced, with a budget of ¥1.67 trillion yuan ($222 billion). This rise was despite underlying economic concerns with high youth unemployment, demand-and-supply problems in the real estate market (fueled by immigration), deflationary pressures, and capital outflows.[18]

---

14 This is based on official annual announcements and external analysis. 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.

15 "Military Expenditure", https://www.sipri.org/research/armament-and-disarmament/arms-and-military-expenditure/military-expenditure, accessed May 30 2023.

16 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/, accessed February 17 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.

17 Defence Expenditures and NATO's 5% commitment, https://www.nato.int/cps/en/natohq/topics_49198.htm (regularly updated), accessed July 4 2025. Whether all NATO members met the 2 percent target is disputed and politically controversial. Jukko Alozious, "NATO's Two Percent Guideline: A Demand for Military Expenditure Perspective", *Defence and Peace Economics*, Vol. 33, Issue 4 (2022), pp. 474–488.

18 Huizhong Wu and Christopher Bodeen, "China Raises Defense Budget by 7.2% as It Pushes for Global Heft and Regional Tensions Continue" (March 5 2024), https://apnews.com/article/china-legislature-defense-budget-taiwan-us-9e751a41c9a1ffe8c0cf9775797750e3. Eswar Prasad, "Wiping Out

Defense spending is often contested and disguised, and raw numbers do not wholly represent the PLA's warfighting potential, including the quality of equipment and quality control.[19] It also cannot account for interoperability of combat forces and integration across the five warfighting domains of air, land, sea, space, and cyber, or the availability of supplies and logistics. Moreover, publicly available data could well be hiding 'black budget' expenditure on undeclared programs.[20] Other warfighting factors are also not straightforwardly measured, including training, the capability to deploy at distance, operational and combat experience, and morale. There are only limited historic conflicts and regional wars several generations ago to draw on for assessment, allied to observations of contemporary Chinese military exercises, performance, and developments.

The PLA was deployed in support of communist forces in the Korean War (1950–1953) and Vietnam War (1963–1973). It also fought a border war with India in 1962 and periodic border skirmishes with the Soviet Union (1969) and Vietnam, including a short war in 1979 (the third Indochina War).[21] The absence of major conflicts means the "PLA remains untested on the modern battlefield" whilst promoting interoperability between its military branches is an ongoing endeavor.[22] Prior to 2015 the size of the PLA was officially estimated at 2.3 million personnel. 73 percent were in the army or Second Artillery Force. However, this was no ordinary "artillery force". It was the strategic missile force for nuclear and conventional rockets. When it was upgraded to the PLA Rocket Force (PLARF) in 2016, it became a full service alongside the army, navy, and air force. Emphasizing the primacy of the army, the PLA Navy (PLAN) in 2016 con-

Bad Data Will Not Solve China's Economic Woes" (February 14 2024), https://www.ft.com/content/4f25f36e-1234-41e3-9d34-a488f8ff631b. Both accessed March 6 2024.

19 Peter Robertson and Wilson Beaver, "China's Defense Budget Is Much Bigger Than It Looks" (September 19 2023), https://foreignpolicy.com/2023/09/19/china-defense-budget-military-weapons-purchasing-power/, accessed September 24 2023.

20 Richard A. Bitzinger, "Just the Facts, Ma'am: The Challenge of Analyzing Chinese Military Expenditures", *China Quarterly*, Vol. 173 (March 2003), pp. 177–193. Adam P. Liff and Andrew S. Erickson, "Demystifying China's Defence Spending: Less Mysterious in the Aggregate", *China Quarterly*, Vol. 216, (March 2013), 805–830.

21 Mark A. Ryan, David M. Finkelstein, and Michael A. McDevitt (eds.), *Chinese Warfighting: The PLA Experience since 1949* (New York: Routledge, 2015).

22 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 232021.

tained around 10 percent of China's armed forces and the PLA Air Force (PLAAF) 17 percent.[23]

Major reforms in 2015 reorganized the PLA and its command-and-control (C^2) structure. This replaced its system of military regions to a theater command structure centrally controlled by the CMC. The previous seven military regions became Eastern, Southern, Western, Northern, and Central theater commands. The PLA's four existing general departments (General Staff, Political, Logistics, and Armament) and army headquarters were reformed, with their previous roles reconstituted in 15 new departments, commissions, and offices overseen by the CMC.[24] According to the U.S. Defense Intelligence Agency (DIA), these reforms and reorganization saw PLA ground forces downsized to under a million.[25]

Correspondingly, the PLA's legacy structures were an inheritance from the Mao and Deng eras. The army remained politically and bureaucratically dominant. This was reproduced through the regional military command structures, none of which was headed by air force or navy officers. This legacy also meant that there was no joint operational command structure, leaving the PLA "out of sync with the changing nature of warfare", leading to the most ambitious shakeup since the 1950s.[26]

In addition, a new Strategic Support Force (PLASSF) was created. Within the PLASSF a new Space Systems Department was also initiated, with the aim of integrating with the five theater commands. In addition, the PLASSF also has a dedicated Network Systems Department which is believed to oversee cyber, electronic warfare/intelligence (ELINT), and "psychological warfare" operations. To promote interoperability, the design is to offer flexibly to the theater commands integrated by the CMC, reflecting the synergy between the five warfighting domains and able to conduct independent operations through separate headquarters/departments.

In addition, it is possible the PLASSF could be used alongside the CMC's Joint Staff Department's (JSD's) Intelligence Bureau (情报局) – previously the General Staff Department (GSD) Second Department (2PLA). One of its priorities is data fusion of all-source intelligence able to be actionably shared in timely sequence. This includes remote sensing, ELINT, surveillance, navigation, and communications and

23 Dennis J. Blasko, "Integrating the Services and Harnessing the Military Area Commands", *Journal of Strategic Studies*, Vol. 39, Nos. 5–6 (2016), pp. 685–708.

24 Blasko, "Integrating the Services", pp. 685–708.

25 DIA, *China Military Power* (2019), p. 55.

26 P.K. Mallick, *China in the Cyber Domain* (New Delhi: Vivekananda International Foundation/ Prints Publications, 2022), p. 72.

intelligence gained through cyberespionage.[27] The JSD is also said to incorporate 1PLA's C^2 recruitment, planning, and administrative bureaus, with its bureau branches in areas including surveys and mapping, metrology, hydrology, and targeting moved to the PLASSF.[28] Reorganization has not remained static. In April 2024, it was announced that the PLASSF would be disbanded or reorganized into the Space Force, Cyber Force, and Information Support Force.[29] Prior to the first major series of Xi-era reforms in 2015, the "focal point" of the PLA's intelligence efforts was contained in the GSD.[30] More broadly, and highly relevant, "China's intelligence apparatus is complex, huge and almost completely opaque to outsiders".[31]

Cadre training and education were boosted from 2015 but the army was cut by 300,000, its influence reduced as part of a wider move to reorient the PLA from a land-based defensive force to one capable of force projection and maritime operations.[32] As yet this has not developed from military operations other than war or coastal defense/offence into blue water capabilities. Nevertheless, these reforms portend a generational shift and an ongoing evolutionary process as the PLA heads to the 100th anniversary of the communist revolution and founding of the PRC in 2049.[33]

The aforementioned Central Military Commission is "the PLA's highest decisionmaking body … technically both a party organ subordinate to the CCP Central Committee and a governmental office appointed by the National People's Congress … staffed almost exclusively by military officers".[34] The CCP's Political Bureau (Politburo), notably including the Politburo Standing Committee, is the apex of this po-

27 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. 218–264. Mallick, *China in the Cyber Domain*, pp.113–115.

28 Mallick, *China in the Cyber Domain*, p. 113.

29 Joe McReynolds and John Costello, "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/planned-obsolescence-the-strategic-support-force-in-memoriam-2015-2024/ and 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.

30 Peter Mattis, "China's Military Intelligence System is Changing" (December 29 2015), https://warontherocks.com/2015/12/chinas-military-intelligence-system-is-changing/, accessed February 21 2024. Cheng, *Cyber Dragon*, pp. 177–197.

31 Mallick, *China in the Cyber Domain*, p. 79.

32 With an admixture of power politics.

33 Noon and Bassler, "Schrodinger's Military?". Blasko, "Integrating the Services", pp. 685–708.

34 DIA, *China Military Power* (2019), p. 14.

litical structure.[35] The National People's Congress, nominally China's representative parliament, is distinctly subordinate to the CCP. In China the party-state is intimately coupled. Senior officers from the PLA "typically have constituted about 20 percent of the CCP's Central Committee".[36] Moreover, since 2012 (under President Xi) China's system of government has become increasingly centralized.[37] The senior leadership often holds multiple positions within China's sprawling bureaucracy.[38] Increasing top-down centralization means the National People's Congress has become more concentrated on governance than representation.[39]

China's air force (PLAAF), navy (PLAN), and rocket force (PLARF) were never autonomous services within the PLA, but since 2015 there have been clear designs to foster a greater degree of increased unity and joint operational synergy between them.[40] How integrated they have become since 2015 remains an ongoing question but to foster increased interoperability, in 2016 the PLA established the Joint Logistics Support Force. One of its aims is to leverage civilian expertise and foster military–civil fusion.[41] Chapters 3 and 4 will show the importance of this fusion in relation to Chinese cyberespionage.

From 2016–2021 domestic commentary on these reforms centered on President Xi's drive to enable the PLA to become a seamlessly integrated joint force. This commentary indicates interservice rivalry (a common issue in militaries), technological issues (another common problem), and ineffective operational commanders. In addition, the army and its leadership remain reluctant to relinquish their position as the senior service. This means that "China still has a long way to go to achieve its [military] ambitions".[42]

China has been a nuclear power since 1964. The majority of China's nuclear forces are land-based missiles (silo based and mobile) housing multiple independently targetable re-entry vehicles. Around 20 bombs are stockpiled for air delivery

35 Cheng, *Cyber Dragon*, pp. 4–7, 42–43, 59.

36 DIA, *China Military Power* (2019), p. 16.

37 Jian Yan and Xuedong Yang, "'Old Brooms Can Still Sweep': The Logic of Furthering CPC's Centralized System", *Journal of Chinese Governance*, Vol. 8, No. 2 (2023), pp. 180–205.

38 See also Jon R. Lindsay, "China and Cybersecurity: Controversy and Context", 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. 7–15.

39 Xuedong Yang and Jian Yan, "Governance Edging Out Representation? Explaining the Imbalanced Functions of China's People's Congress System", *Journal of Chinese Governance*, Vol. 6, No. 1 (2021), pp. 110–130.

40 Cheng, *Cyber Dragon*, pp. 18–36.

41 Caitlin Campbell, "China's Military: The People's Liberation Army (PLA)" (June 4, 2021), pp. 42–46, https://crsreports.congress.gov/product/pdf/R/R46808, accessed November 7 2021.

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

by Xian H-6 bombers (Chinese-purchased Russian Tu-16 "Badgers"). A number are also available to its four 094-class (Jin) ballistic missile submarines (SSBNs). It is believed that the CMC does not allow nuclear warheads to be deployed on missiles, including submarine launched ballistic missiles (SLBMs), during peacetime.[43] It was estimated in mid-2024 that China's nuclear stockpile amounted to 600 operational warheads. This is projected to rise after 2030.[44]

The SSBNs carry JL-2 SLBMs with a 7,200 km range but because China's SSBNs are "not yet conducting regular open-ocean patrols" they do not have the range to reach the continental United States. Instead, they are believed to patrol near Chinese coastal waters protected by a combination of hunter-killer submarines (SSNs), surface vessels, and other anti-access area denial forces and capabilities. China is meanwhile looking to develop quieter submarines, and foreign submarine (and other maritime) technology is one of China's (cyber)espionage targets.[45]

2 China's rise

Between 1943 and 1976, under Chairman Mao Zedong, the PRC began a "Great Leap Forward" aimed at modernizing the largely agrarian economy of China. This "Great Leap Forward" also contributed to widespread famine.[46] Mao also began the Cultural Revolution in 1966 which aimed to solidify power in the CCP and his leadership.[47] By the time of his death in 1976 it proved "so great a disaster that it provoked an even more profound cultural revolution", with his ultimate successor Deng Xiaoping striving "to abandon this vain search for a Chinese version of modernity" and "jump on the bandwagon of successful Western-style mod-

43 Hans M. Kristensen and Robert S. Norris, "Chinese Nuclear Forces, 2018", *Bulletin of the Atomic Scientists*, Vol. 74, No. 4 (August 2018), pp. 289–295.

44 Shizuka Kuramitsu, "Pentagon Says Chinese Nuclear Arsenal Still Growing" (January/February 2025), https://www.armscontrol.org/act/2025-01/news/pentagon-says-chinese-nuclear-arsenal-still-growing, accessed 5 July 2025.

45 Anonymous, "The Survivability of China's SSBNs and Strategic Stability" (October 24 2018), https://admin.carnegieendowment.org/2018/10/24/survivability-of-china-s-ssbns-and-strategic-stability/jzdy, accessed October 23 2021.

46 Roderick MacFarquhar, *The Origins of the Cultural Revolution, Volume 2* (New York: Columbia University Press, 1983).

47 Roderick MacFarquhar and Michael Schoenhals, *Mao's Last Revolution* (Cambridge, MA: Harvard University Press, 2006). The Cultural Revolution is also documented in Jung Chang's first-hand account, *Wild Swans: Three Daughters of China 25th Anniversary Edition* (London: Harper Collins, 2016).

ernization".[48] Reform and opening the "bamboo curtain" under Deng in the late 1970s were keys that helped unlock the Chinese economy as the Cold War ended. This saw "Four Modernizations" in agriculture, industry, defense, and science and technology. The collectivization of agriculture was rolled back as China turned towards capitalism and the free market.[49] Deng's legacy stands comparison with the similarly minded Mikhail Gorbachev.[50]

The fractious period under Chairman Mao had also seen the Sino-Soviet split and the beginnings of opening China to foreign investment and export-led growth. Although the PLA became a stronger force in the wake of the Cultural Revolution it was still not in the ranks of a great power and was dwarfed by the two superpowers.[51] The upheaval of the Cultural Revolution and the end of the Cold War saw China prioritize other aspects of development. It took until the early 1990s for China to concentrate focus on the PLA's military capabilities. Since then, the PLA has transformed from a low-tech, land-based, defense-oriented force into one that is increasingly capable of force projection, enabled by its navy and space assets. This has helped the PRC claim and protect (frequently disputed) territories in the South China Sea and secure its supply lines. In the post-Cold War world, the CCP was determined not to repeat the "so-called Century of Humiliation covering the period from the mid-19th century up to the founding of the People's Republic in 1949 during which China was virtually colonised by the west".[52]

New learning also took place during Deng's two decades of office. Most especially, China began to open its doors to the outside world. This contributed to pressures building for political reforms in the late 1980s prior to the 1989 counterrevolutionary/pro-democracy crackdown culminating at Tiananmen Square. This followed sweeping protests in Eastern Europe which had toppled communist regimes across the region and would soon end the Soviet Union. Whilst economic liberalization would continue so would the rule of the CCP. There would be no

48 MacFarquhar and Schoenhals, *Mao's Last Revolution*, pp. 3 and 460.

49 Tony Walker, "'To Get Rich Is Glorious': How Deng Xiaoping Set China on a Path to Rule the World" (July 9 2021), https://theconversation.com/to-get-rich-is-glorious-how-deng-xiaoping-set-china-on-a-path-to-rule-the-world-156836, accessed March 11 2024.

50 Shiping Hua, "The Deng Reforms (1978–1992) and the Gorbachev Reforms (1985–1991) Revisited: A Political Discourse Analysis", *Problems of Post-Communism*, Vol. 53, No. 3 (May/June 2006), pp. 3–16.

51 DIA, *China Military Power* (2019), p. 2.

52 Nigel Inkster, "China's Strategy to Become the World's Strongest Cyber Power: Nigel Inkster, Former Operations and Intelligence Director of MI6, Analyses China's Efforts to Impose Order on Its Vast Online Community" (February 23 2017), https://www.newstatesman.com/microsites/cyber/2017/02/china-s-strategy-become-world-s-strongest-cyber-power, accessed July 1 2019.

move to multi-party democracy in China.[53] These two pillars have remained constant under Jiang Zemin (1989–2002), Hu Jintao (2002–2012), and, since 2012, Xi Jinping. The dissolution of the USSR also made the PRC more secure.[54] Under Xi, China has "formalized three broad goals for the PLA": (1) to accomplish mechanization of the PLA with "networked" capabilities by 2020; (2) to "basically complete" PLA military modernization by 2035; and (3) to have a "world-class" military by the time of the PRC'S centenary in 2049.[55]

3 Economically liberal, politically closed: Chinese "cyberwarfare" and strategic culture

Although the CCP liberalized to allow people more freedom after Tiananmen Square in 1989, the PRC is not an open society in the Western sense. However, like many other large nations, it is a multiethnic empire with regional differences.[56] Moreover, despite elements of China's military development being publicized or increasingly visible, interpreting unclassified thinking on the issues of what the West sees as cyberespionage and "cyberwarfare", including pronouncements from senior political and military leaders, is challenging. This is also reflected in the nature and substance of their ongoing efforts to restructure the PLA. This is through books, articles, conferences, speeches, and official government documents by former and serving members of the CCP and PLA, through China's involvement with the second edition of the Tallinn Manual, and academic discourse. This said, whilst declaratory policy papers are useful, they also need healthy skepticism (especially as one of their audiences is China watchers abroad). Western commentary and analysis abound.

Visibility is also evident in China's cyberespionage campaigns, especially those publicly exposed. These provide empirical indicators of targets and capabilities. However, what is contested and obfuscated is what its long-term strategy is for the use of cyber as a standalone (or incorporated) attack vector and how this integrates with hard military power across the four other recognized domains of land, sea, air, and space. This book seeks to improve visibility and line of sight on these issues.

---

53 John P. Burns, "China's Governance: Political Reform in a Turbulent Environment", *China Quarterly*, No. 119 (September 1989), pp. 481–518.

54 Cheng, *Cyber Dragon*, p. 23.

55 Campbell, "China's Military: The People's Liberation Army (PLA)", Summary.

56 Thomas G. Mahnken, *Secrecy and Stratagem: Understanding Chinese Strategic Culture* (Double Bay, NSW: Lowy Institute for International Policy, 2011), p. 15.

Western analysis of PRC strategy, and the stratagems it employs, can suffer from problems of "mirror imaging" (seeing the other side as you see yourself) with similar motivations. Classified (and therefore unknown capabilities and designs) alongside problems with translating Mandarin Chinese (spoken in 70 percent of China) and the concepts they capture into the English language and Western lexicon form part of this mirror imaging.[57] This is important, as is understanding China and appreciating Chinese culture in all its forms (as much as practicable). This includes Chinese strategic culture.[58]

A supplement to mainstream international relations theories, strategic culture is reflected in the writings of Sun Tzu and Clausewitz.[59] Understanding strategic culture can potentially help generate insights into the subject matter of this book by appreciating China's history, and its national, regional, and cultural journey. Viewed through this lens, its distinctiveness in approach, informed by philosophical traditions and China's political and cultural history pre- and post-1949, can be enlightened. It can also illuminate how the opinions and cognitive characteristics of state structures, leadership character, theorems and strategizing, and how its national and international approaches, have formed and been shaped over time. This does not mean that states and actors like China are bound by history to follow a predetermined course of action, but that strategic culture can play a part in approaches, decisions, and actions. Nor does it mean that strategic culture is fixed in time. These structural approaches embrace agency in strategic choices taken by the PRC's politico-military leadership.[60] Moreover, geographic origins and geographic diversity also impact the make-up and formation of strategic sub-cultures within a state, especially one as large and diverse as China.

What it does suggest is that culture can guide outlook, thought processes, and decisionmaking. This produces variation. It can also lead to contested views. In re-

---

57 Amy Chang, "Warring State: China's Cybersecurity Strategy", Center for a New American Security, December 2014, https://www.cnas.org/publications/reports/warring-state-chinas-cybersecurity-strategy, accessed April 9 2019. Mandarin is the universal language of writing and communication within the military, as well as ancillary scholarship.

58 The origins of strategic culture from an international relations perspective can be traced back to Jack Snyder, *The Soviet Strategic Culture: Implications for Limited Nuclear Operations* (Santa Monica, CA: Rand, 1977).

59 Ted Hopf, "The Promise of Constructivism in International Relations Theory", *International Security*, Vol. 23, No. 1 (Fall 2000), pp. 171–200. Alexander Wendt, *Social Theory of International Politics* (Cambridge: Cambridge University Press, 1999). Dale C. Copeland, "The Constructivist Challenge to Structural Realism: A Review Essay", *International Security*, Vol. 25, No. 2 (Fall 2000), pp. 187–212.

60 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.

spect to China, there are two aspects of Chinese strategic culture that appear to be accepted amongst Western Sinologists: a "parabellum" (realist/realpolitik) and a "Confucian-Mencian" strand. The latter, drawing on the philosophy and traditions established by Confucius and later adherents, is defensive in nature, guided by morality, and non-expansionist.[61] The former is prepared to use force, reflecting both classical realism (founded on power politics and the use of force[62]) and neoclassical realism (through which foreign and security/defense policy can be constrained by structural and institutional factors in the international system).[63] In the PRC, they are not mutually exclusive nor are they viewed as at odds with one another.[64] This includes through Confucian beliefs which influence what the West calls the "Just War Tradition".[65] This includes a just war that embraces offensive strategies (arguably seen through both liberal/neo-liberal and realist mindsets in Chinese culture). It also embraces Marxist-Leninist beliefs on class-based aspects of war and their influence upon Mao's "People's War".[66]

All these elements are important to better understand the strategic culture of the CCP and PLA, their policy choices, cyber campaigns, and their capabilities and operations (without seeing it as a template for choices). The theories underlying the activities of the PRC are valuable in these respects. Timothy L. Thomas of the U.S. Foreign Military Studies Office attested in 2012: "analysts should be concerned about the pace of China's cyber developments as PLA theoreticians attempt to establish the groundwork to achieve a strategic cyber advantage over potential

---

61 Huiyun Feng, *Chinese Strategic Culture and Foreign Policy Decision-Making: Confucianism, Leadership and War* (New York: Routledge, 2007).

62 Perhaps best summed up by the Melian dialogue of Thucydides ("the strong do what they can, the weak suffer what they must"). Steven Forde, "Varieties of Realism: Thucydides and Machiavelli", *Journal of Politics*, Vol. 54, No. 2 (May 1992), pp. 372–393.

63 Steven Forde, "International Realism and the Science of Politics: Thucydides, Machiavelli, and Neorealism", *International Studies Quarterly*, Vol. 39, Issue 2 (June 1995), pp. 141–160. Michael C. Williams, "Why Ideas Matter in International Relations: Hans Morgenthau, Classical Realism, and the Moral Construction of Power Politics", *International Organization*, Vol. 58, Issue 4 (Fall 2004**),** 633–665.

64 Alastair Iain Johnston, "Thinking about Strategic Culture", *International Security*, Vol. 19, No. 4 (Spring 1995), pp. 32–64. Alastair Iain Johnston, *Cultural Realism: Strategic Culture and Grand Strategy in Chinese History* (Princeton, NJ: Princeton University Press, 1995). Andrew Scobell, "China's Real Strategic Culture: A Great Wall of the Imagination", *Contemporary Security Policy*, Vol. 35, No. 2 (2014), pp. 211–226. Andrew Scobell, *China's Use of Military Force: Beyond the Great Wall and the Long March* (New York: Cambridge University Press, 2003).

65 Nicholas Rengger, "On the Just War Tradition in the Twenty-First Century", *International Affairs*, Vol. 78, Issue 2 (April 2002), pp. 353–363.

66 Tiewa Liu, "Chinese Strategic Culture and the Use of Force: Moral and Political Perspectives", *Journal of Contemporary China*, Vol. 23, No. 87 (2014), pp. 556–574.

adversaries".[67] That groundwork was successful and essential. More than a decade later, analysts should perhaps be more concerned with the extent and development of Chinese cyber campaigns (as well as ongoing theorization). James Mulvenon indicated back in 2009, China's "interest in the full spectrum of computer network attack tools, including hacking, viruses, physical attack, insider sabotage, and electromagnetic attack".[68] This had antecedents dating to the end of the Cold War.

4 China's military rise: the 1991 Gulf War and the genesis of PLA thinking on "cyberwar"

The First Gulf War of 1991, the first major conflict that took place as the Cold War was ending, began to usher in a change in PLA thinking regarding the usefulness and uses of Information Communications Technology (ICT) in modern conflict. The PLA took several lessons from the First Gulf War but primarily how technological advantage was decisive in achieving rapid military victory. It was noted not only that precision-guided munitions comprised just 7 percent of all weapons used by the U.S. in the 1991 Gulf War, but also that these destroyed 80 percent of vital targets. Also noted was how intelligence was utilized in achieving rapid and decisive victory over Iraqi forces in the liberation of Kuwait. This included satellite reconnaissance and satellite communications allied to ELINT and human intelligence (HUMINT).[69]

To this point the PRC had seen sheer manpower as their main advantage. Since the civil war, Chinese strategic culture had "emphasized the importance of people, not equipment, in warfare and employed massed forces or weapons – the strengths China brought to bear in the Korean War, the Sino-Indian War, and the Sino-Vietnam War".[70] During the Mao era, the U.S. DIA indicated how Chinese forces were geared to fight a war more akin to World War II. This rested on prioritizing defense of the homeland and "luring an enemy into China to fight a

67 Timothy L. Thomas, *Three Faces of the Cyber Dragon: Cyber Peace Activist, Spook, Attacker* (Fort Leavenworth, KS: Foreign Military Studies Office, 2012), p. 7.

68 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), p. 277.

69 Peng Guangqian and Yao Youzhi (eds.), *The Science of Military Strategy* (Beijing: Military Science Press, 2005), p. 337. Quoted in Larry M. Wortzel, *The Chinese People's Liberation Army and Information Warfare* (Carlisle, PA: United States Army War College Press, 2014), p. 5.

70 Wortzel, *The Chinese People's Liberation Army and Information Warfare*, p. 5.

'people's war' with regular troops, irregular (guerrilla) forces, and the general populace".[71]

This "Maoist paradigm" would change. China's official military strategy of 2015 recorded that, since 1993, China had been adopting new military strategic guidelines. These "took winning local wars in conditions of modern technology, particularly high technology, as the basic point in making preparation for military struggle".[72] In 2004, these guidelines were substantiated and modified to be able to fight and win "local wars" under conditions of informationization.[73] Informationization (*xinxihua*/ 信息化) included Network Warfare (网络战争) and Information Warfare (*xinxizhan*) and increasing technological integration to the battlefield.[74] This would enable the PLA to "press forward ... [and] shift ... the focus of war mobilization from human resources to science and technology".[75] This has wider applications drawn from the ICT revolution that was permeating the PRC at the same time as in the West and wider world.[76]

In the years between the First Gulf War and today, China has been a rising power. Chris Demchak of the U.S. Naval War College sets this in context:

> In the 1980s, the former leader of China Deng Xiaoping predicted China would equal the US as a global great power over a period of roughly 70 years because of its demographic and economic weight in the global system ... By most measures, the rise of China was inevitable but

71 DIA, *China Military Power* (2019), pp. 2–3.

72 "Full Text: China's Military Strategy (Xinhua)" (May 26 2015), http://www.chinadaily.com.cn/china/2015-05/26/content_20820628_3.htm, accessed February 1 2019. Or http://eng.mod.gov.cn/Press/2015-05/26/content_4586805.htm.

73 On the concept of "informization" see Joe McReynolds and James Mulvenon, "The Role of Informization in the People's Liberation Army under Hu Jintao", in Roy Kamphausen, David Lai and Travis Tanner (eds.), *Assessing the People's Liberation Army in the Hu Jintao Era* (Carlisle, PA: Strategic Studies Institute and U.S. Army War College Press, 2014), pp. 207–256.

74 China's official English-language translation of their defense white papers renders the term *xinxihua* as "informationization". However, U.S. government documents spell it as "informatization". The terms appear to be interchangeable as "informationization" or "informatization". The author is grateful to one of the anonymous peer reviewers of this book for this insight. *Xinxihua* has been noted as a cognate for "cyber" in the Chinese lexicon. Timothy L. Thomas, "Nation-State Cyber Strategies: Examples from China and Russia", in Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (eds.), *Cyberpower and National Security* (Washington DC: University of Nebraska Press, Potomac Books, 2009), chapter 20. Available from https://ndupress.ndu.edu/Portals/68/Documents/Books/CTBSP-Exports/Cyberpower/Cyberpower-I-Chap-20.pdf?ver=2017-06-16-115054-850, accessed November 24 2024. "APT1: Exposing One of China's Cyber Espionage Units" (2013), p. 52, https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf, accessed January 16 2019.

75 "Full Text: China's Military Strategy (Xinhua)" (May 26 2015).

76 Cheng, *Cyber Dragon*, pp. 1–17.

> has occurred faster than anticipated. Analyses … predicted parity would occur by 2025, with [China's economy] doubling that of the US by 2050. As of this writing [2017], various authors argue that China has been roughly at parity for several years (at least since 2014).[77]

Many in the West are fearful of China's rise. U.S. Congressional debates regularly feature warnings of growing Chinese "soft power" influences and increasing use of "hard power" backed by military modernization programs across the domains of land, sea, air, space, and cyber.[78] This is most evident in a theory that China, as a rising power, and America, as a dominant power, might be destined for conflict. This is referred to as "Thucydides' Trap".[79] But, as General Michael Hayden, the former Director of both the Central Intelligence Agency (CIA) and National Security Agency (NSA), has argued, whilst "The Chinese … are growing in power … I'm not reflexive on attaching malevolent intent to everything the Chinese do. A whole bunch of what it is that they do are the natural things for nations in their circumstances."[80]

5 PLA reforms and restructuring PRC Security Ministries

The General Staff, the equivalent of the U.S. Joint Chiefs of Staff, oversees the PLA. Peter Mattis, a former CIA officer, wrote in 2012 how China's military intelligence was then organized through the General Staff Department. The GSD was the locus for all-source intelligence. At that point, how PLA intelligence fusion was being

---

77 "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.

78 Department of Defense, *Annual Report to Congress: Military and Security Developments involving the People's Republic of China 2018*, https://media.defense.gov/2018/Aug/16/2001955282/-1/-1/1/2018-CHINA-MILITARY-POWER-REPORT.PDF, accessed April 9 2019. On China's conventional military strength see DIA, *China Military Power* (2019).

79 Graham Allison, *Destined for War: Can America and China Escape Thucydides' Trap?* (New York: Houghton Mifflin Harcourt, 2017).

80 Thomas Macaulay, "Former Bosses of CIA, MI6 and DHS Compare Cyber Threats of Russia and China: The Former Spy Chiefs Examined Russia's Cyber Attacks on the US and Global Developments in Cyberwarfare at Oracle OpenWorld" (October 26 2018), https://www.techworld.com/security/cia-mi6-dhs-ex-bosses-compare-cyber-threats-of-russia-china-3685790/, accessed February 3 2019.

conducted was (and remains) opaque. Mattis questioned how the GSD department system functioned in terms of intelligence collection, processing, and dissemination. Questions were also raised regarding how the GSD was processing the vast increases in data and information flows enabled by the evolution of the Internet and associated ICT. Insight into this was a prerequisite for the U.S. Intelligence Community (USIC) to help policymakers signal and communicate to their Chinese counterparts.[81] Over a decade later much more is becoming known, but open-source intelligence (OSINT) analysis and classified intelligence analysis still leave room for interpretation.

The PLA is responsible to the CCP not the Chinese state. The PLA houses substantial and sizeable intelligence capacity. This naturally changes over time and the indications are that its trajectory is only upwards. Provincial governments were in 2015 said to have extensive de facto autonomy over intelligence whilst fiercely competing for patronage.[82] Western analysis indicated little distinction between internal security policies and intelligence from an institutional perspective. What was known about the organizations themselves and their importance to Chinese policy was limited. However, intelligence was believed "not just part of a policy staff process but an integral tool for the preservation of the power of the Chinese Communist Party".[83] Much more is now known, but the granular details and changes over time still have many question marks against them.

The GSD Second Department now operates as the Intelligence Bureau of the Joint Staff Department under the CMC. It is responsible for HUMINT collection and oversees the work of defense attachés operating from China's embassies as well as related clandestine activities.[84] It is believed that the GSD Third Department (3PLA), controlling Signals Intelligence (SIGINT), and GSD Fourth Department (4PLA), responsible for ELINT and offensive "electronic warfare", were subsumed into the PLASSF. This is discussed in chapter 2.[85] Part of their SIGINT collection and

81 Peter Mattis, "Beyond Spy vs. Spy: The Analytic Challenge of Understanding Chinese Intelligence Services", *Studies in Intelligence*, Vol. 56, No. 3 (September 2012), p. 48.

82 Jon R. Lindsay, "The Impact of China on Cybersecurity: Fiction and Friction", *International Security*, Vol. 39, No. 3 (Winter 2014/15), p. 18.

83 Mattis, "Beyond Spy vs. Spy", p. 47.

84 STRATFOR's March 2010 assessment was this work was previously undertaken by the MSS and that the "FBI believes there could be hundreds of thousands of individuals and as many as 3,000 front companies operating in the United States alone". STRATFOR, "Intelligence Services, Part 1: Espionage with Chinese Characteristics" (March 2010), p. 5, See also pp. 9–11 on Chinese military intelligence. https://wikileaks.org/gifiles/attach/133/133464_INTEL_SERVICES_CHINA.pdf, accessed June 28 2019.

85 DIA, *China Military Power* (2019), pp. 99–100.

capacity community were located in at least 28 technical reconnaissance bureaus (TRBs).

3PLA also had control over 12 operational bureaus, 3 research institutes, and 1 computing center. Eight of those 12 operational bureau headquarters were clustered in Beijing. Two more were based in Shanghai, with one in Qingdao and the other in Wuhan. In addition, 10 TRBs provided direct support to the PLA's seven military regions. A further 6 were tasked with supporting the PLAN, PLAAF, and the Second Artillery Force (PLASAF), now the Rocket Force. The Second Bureau (including Unit 61398 – discussed below) is among the largest of the 12 operational bureaus that comprised 3PLA.[86]

The CCP also controls the Ministry of State Security (MSS), the Ministry of Public Security (MPS), and the system of Public Security Bureaus and People's Armed Police (which was overseen by the MPS but came under the purview of the CMC in 2020). It also controls Communist Party apparatus including the Central Propaganda Department.[87] The MPS is responsible for policing, including the investigation of domestic corruption, the maintenance of social stability, and Internet monitoring, as well as supporting the MSS in counterintelligence.[88] The MPS, sometimes described as China's FBI, had by 2015 established bilateral law enforcement cooperation with over 30 countries. This includes the United States, United Kingdom, Germany, and Russia. It aided over 50 countries in investigating more than a thousand cases of cybercrime from 2005–2015.[89] Among the issues China faces are common international problems. This includes organized crime, including pyramid scams, drug trafficking, and the smuggling of illicit goods. They also investigate

86 Mark A. Stokes, "The PLA General Staff Department Third Department Second Bureau: An Organizational Overview of Unit 61398", Project 2049 Institute (July 27 2015), pp. 3–4, https://project2049.net/2015/07/27/the-pla-general-staff-department-third-department-second-bureau-an-organizational-overview-of-unit-61398/, accessed April 8 2019. Mark A. Stokes, "The Chinese People's Liberation Army Computer Network Operations Infrastructure", in Lindsay et al., *China and Cybersecurity*, pp. 163–187.

87 Ministry of National Defense of the PRC, "Law of the People's Republic of China on the People's Armed Police" (2020), http://eng.mod.gov.cn/xb/Publications/LR/4888359.html, accessed November 24 2024. Wortzel, *The Chinese People's Liberation Army and Information Warfare*, p. 18. Tobias Feakin, "Enter the Cyber Dragon: Understanding Chinese Intelligence Agencies' Cyber Capabilities", https://www.files.ethz.ch/isn/165376/10_42_31_AM_SR50_chinese_cyber.pdf, Australian Strategic Policy Institute Special Report, Issue 50 (June 2013), pp. 3–4.

88 STRATFOR, "Intelligence Services, Part 1: Espionage with Chinese Characteristics" (March 2010), p. 4.

89 Joe McReynolds, "China's Evolving Perspectives on Network Warfare: Lessons from the Science of Military Strategy" *China Brief*, Vol. 15, Issue 9 (April 16 2015), https://jamestown.org/program/chinas-evolving-perspectives-on-network-warfare-lessons-from-the-science-of-military-strategy/#.V1BM2_krK70, accessed February 3 2019.

cases of child pornography, online theft, fraud, extortion (ransomware), and money laundering.[90]

International cooperation in these areas of crime/cybercrime notwithstanding, Chinese nationals, including many alleged to work for the MSS and MPS, also appear on the Federal Bureau of Investigation's (FBI's) "Cyber Most Wanted" list for cyber-enabled crimes.[91] As chapters 3 and 4 will show, a great deal of these charges stems from intellectual property theft through cyberespionage (sometimes aided by traditional espionage and spycraft). Espionage/cyberespionage operations include "multi-year intrusion campaigns targeting highly sensitive economic, proprietary, or national security information" which the cybersecurity world characterizes as Advanced Persistent Threats (APTs).[92] APT cyberespionage campaigns may be directed from the political center or leadership of intelligence agencies, but they are operationally undertaken by hackers and field agents in mainland China and abroad. These agencies include Unit 61398 (now believed subsumed into the PLASSF).[93] If these operations have in-country agents working for (or working with) the PLA or MSS they run a greater risk of discovery and can (and sometimes have) faced prosecution.

6 Chinese cyberespionage prior to 2015: 3PLA, 4PLA, and the TRBs

The base of 3PLA in Shanghai described above also housed/houses government research institutes and technology companies. Its base includes the main building (commissioned in 2003). Part of this industrial compound also contains (or contained) the MPS's Third Research Institute conducting research into digital foren-

90 "Fighting Organized Crime in China", https://www.interpol.int/en/Who-we-are/Member-countries/Asia-South-Pacific/CHINA. "Building Cyberspace Community with a Shared Future: Promoting Cooperation against Cybercrime", C.S.D, The Ministry of Public Security of P.R.C. Zhang Gangqiang (July 2020), https://www.unodc.org/documents/Cybercrime/Presentations/CHINA_International_cooperation.pdf. Both accessed February 28 2024.

91 "Cyber's Most Wanted", https://www.fbi.gov/wanted/cyber, accessed February 28 2024.

92 Eric Hutchins, Michael Cloppert, and Rohan Amin (Lockheed Martin), "Intelligence-Driven Computer Network Defence Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains", in Julie Ryan (ed.), *Leading Issues in Information Warfare and Security Research, Volume 1* (Reading: Academic Publishing International, 2011), p. 81.

93 On Chinese capabilities and structure see for example Nigel Inkster, "China's Cyber Power", *Adelphi*, Vol. 55, Issue 456 (2015), pp. 51–82.

sics and network security.[94] It has also been speculated that the 3PLA evolved from purely SIGINT to lead China's defensive efforts in information assurance (part of what the U.S. Department of Defense characterizes as Computer Network Defense. It also conducts intelligence preparation of the battlefield (Computer Network Exploitation).[95]

As well as signals collection (SIGINT), 3PLA was also responsible for communications security for the PLA, technology reconnaissance, and its exploitation and analysis.[96] This is why it has often been compared to the NSA.[97] Prior to the 2015 reorganizations, 3PLA might have been home to as many as 130,000 linguists, engineers, technicians, analysts, and researchers. It drew data from instrumented ships, tactical mobile ground systems, airborne platforms, and a system of several dozen ground stations.[98]

The TRB system supports these intelligence collection and exploitation activities. The TRBs were subordinate to 3PLA and helped monitor foreign communications and cyberespionage. Each of China's military regions had at least one TRB assigned to it through its headquarters. So did the PLAAF, PLAN, and PLASAF.[99] 3PLA had offices and TRBs in several major cities as well as each of China's military regions (pre-2015). This might well have led to regional differences in approach and analysis.[100] Assessments indicated the TRBs were tasked with SIGINT collection and other Computer Network Operations. Each would have focused on a distinct area of geographic interest to the PLA.[101]

It is believed the 4PLA was mainly responsible for Computer Network Attack planning during peacetime. 4PLA would have potentially become the "trigger pul-

---

94 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.

95 Mulvenon, "PLA Computer Network Operations", p. 274.

96 Bryan Krekel with George Bakos and Christopher Barnett, *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*, prepared for the U.S.–China Economic and Security Review Commission (McLean, VA: Northrop Grumman Corp., 2009), pp. 30–32. Available from https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-030.pdf, accessed April 16 2019.

97 Wortzel, *The Chinese People's Liberation Army and Information Warfare*, p. 21.

98 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), p. 47, https://info.publicintelligence.net/USCC-ChinaCyberEspionage.pdf, accessed April 16 2019.

99 Wortzel, *The Chinese People's Liberation Army and Information Warfare*, p. 22.

100 Mattis, "The Analytic Challenge of Understanding Chinese Intelligence Services", p. 53.

101 Krekel, Adams, and Bakos, *Occupying the Information High Ground*, p. 49.

lers" at both regional and national levels in wartime.[102] Two separate reports by Northrop Grumman in 2009 and 2012 also suggest that 4PLA had responsibility for offensive cyber operations.[103] Larry Wortzel has speculated that whilst 4PLA collected SIGINT and Cyber Intelligence, it was 3PLA, with their analytical and language capabilities, analyzing and exploiting it.[104] Northrop Grumman believed this synergy was consolidated in 2002 after a "hard won" and "prolonged bureaucratic struggle" after which Major General Dai Qingmin (a key figure in chapter 1) assumed control of 4PLA in 2002. There, Dai championed the Integrated Network and Electronic Warfare (INEW) approach he helped conceptualize.[105] Meanwhile, Mallick suggests that the headquarters of 4PLA were elevated to better enable joint INEW operations (Information Warfare and Electronic Warfare) which saw 4PLA brigades incorporated into the PLASSF.[106]

The TRBs might become incorporated into the post-2024 Cyber Force (closely linked to supporting the Space Force) and supporting the theater commands in both peacetime and wartime operations (for offensives and an increasing focus on defense). Base 111 (Unit 61716), directed against Taiwan (also known as the "Three Warfares" base), also appears to be subsumed into the PLA's Network Systems Department which commands cyber, electronic, and psychological warfare.[107]

7 Unit 61398

PLA Unit 61398, previously part of the Second Bureau, was one of the largest of the 12 operational bureaus comprising the 3PLA.[108] It remains unclear whether Unit 61398 was subsumed into the PLASSF after 2015 or was an attempt to obscure its activities. Its physical infrastructure remains, even if its visibility and activities have decreased since 2015. The origins of Unit 61398 have been traced to the Second Bureau and GSD Third Department Fourth Bureau in the mountains west of the Shanxi provincial city of Xinzhou (subsequently relocated to Shanghai in

102 Mulvenon, "PLA Computer Network Operations", p. 274.
103 Krekel, Adams, and Bakos, *Occupying the Information High Ground*, pp. 45–55.
104 Wortzel, *The Chinese People's Liberation Army and Information Warfare*, p. 22.
105 Krekel, Adams, and Bakos, *Occupying the Information High Ground*, p. 48.
106 Mallick, *China in the Cyber Domain*, pp. 110–112.
107 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.
108 Stokes, "The PLA General Staff Department Third Department Second Bureau", p. 4.

1986).[109] Mandiant's 2013 report, "APT1 Exposing One of China's Cyber Espionage Units", went into detail.

Part of Unit 61398 is situated on Datong Road (大同路) in Gaoqiaozhen (高桥镇), in the Pudong New Area (浦东新区) of Shanghai (上海). The central building in this industrial zone compound is a purpose-built 130,663ft^2 facility, 12 stories high, completed in early 2007.[110] This is where Unit 61398 (APT1) operates from. According to Mandiant, it has been there since at least 2006. Unit 61398/APT1 is one of over 20 APT groups known to operate from China and "one of the most prolific cyber espionage groups in terms of the sheer quantity of information stolen".[111] Despite growing capabilities, Kevin Mandia reasoned in 2013 that so far China had operated under Rules of Engagement aimed only at IP theft and not destruction of data or cyber-kinetic destruction.[112] Whilst covertly filming for a follow-up story on Mandiant's report, a CNN crew were chased away from the building in Gaoqiaozhen by PLA officers.[113] The BBC's Beijing correspondent who was with them reported:

> We were stopped pretty promptly from filming. We were briefly detained by the military personnel on the gates, taken inside the base and they refused to let us go until we had agreed to surrender our tape. The Reuters news agencies were able to pick up some footage, and you can see from those pictures that this is a pretty nondescript building. Certainly it doesn't look likely to be the nerve centre of one of the most effective and prolific cyber warfare operations ever mounted.[114]

Mandiant was able to identify three of the individuals responsible for APT1 operating as part of four large networks out of Shanghai. It has been common for cybersecurity firms such as Mandiant not to attribute APTs and cyberespionage campaigns to nations, but in this case Mandiant felt by going public it could induce them to "change their behaviors but first we're giving them a Mike Tyson uppercut".[115]

---

109 Stokes, "The PLA General Staff Department Third Department Second Bureau", p. 4.

110 "APT1: Exposing One of China's Cyber Espionage Units", p. 3.

111 "APT1: Exposing One of China's Cyber Espionage Units", p. 2.

112 "Cracking Down on Chinese Hackers" (February 19 2013), https://edition.cnn.com/videos/bestoftv/2013/02/20/tsr-intv-china-hackers-mandia.cnn, accessed April 23 2019.

113 Zoe Li, "What We Know about the Chinese Army's Alleged Cyber Spying Unit" (May 20 2014), https://edition.cnn.com/2014/05/20/world/asia/china-unit-61398/index.html, accessed April 23 2019.

114 Adam Taylor, "Reporters Detained for Trying to Film Alleged Nerve Center of Chinese Hacking" (February 19 2019), https://www.businessinsider.com/pla-unit-61398-reporters-detained-2013-2?r=US&IR=T, accessed April 24 2019.

115 "Cracking Down on Chinese Hackers" (February 19 2013).

Mandiant attributed APT1 by calling it out through its Military Unit Cover Designator , as Unit 61398 (directed by the CCP).[116] Mandiant reported that the vast bulk of Unit 61398's activities are concentrated upon the United States, with the expertise and capacity to perform cyberespionage against swathes of industries and sectors continually and simultaneously.[117] Based on an analysis of its main building, the technical infrastructure, and associated facilities, Mandiant estimated that Unit 61398 might be staffed by thousands of people trained in cybersecurity, all of whom are proficient in English.[118] This is despite a shortfall of trained cybersecurity professionals in China (estimated at between 700,000 – 1.4 million).[119] It also appears to be an intelligence-led operation as the front-line cybersecurity team of APT1 requires direct on-call support from malware authors, industry experts, OSINT research, and linguists. These then "translate task requests from requestors to the operators, and … transmit stolen information to the requestors".[120]

8 The Ministry of State Security

The MSS, established in 1983, is China's primary civilian intelligence and counterintelligence service whose primary public function is dealing with domestic security and social stability.[121] Its main focus is said to be to combat the "three evils": separatism, terrorism, and religious extremism.[122] It is the main civilian foreign intelligence service, reporting to only the most senior governmental decisionmakers. These are the premier/president, State Council, and the CCP and its Political and Legislative Affairs Committee. The MSS operates countrywide but is headquartered in the Haidian district of Beijing. In common with many other nations, all foreign and domestic intelligence organizations feed intelligence into this central-

116 "APT1: Exposing One of China's Cyber Espionage Units", pp. 3, 7.

117 "APT1: Exposing One of China's Cyber Espionage Units", pp. 21 – 22.

118 The scale and potential numbers are borne out in Stokes, "The PLA General Staff Department Third Department Second Bureau", p. 4.

119 Mallick, *China in the Cyber Domain*, pp. 122, 203 – 221.

120 "APT1: Exposing One of China's Cyber Espionage Units", p. 5.

121 Xuezhi Guo, *China's Security State: Philosophy, Evolution, and Politics* (Cambridge: Cambridge University Press, 2012), p. 437.

122 Nigel Inkster, "The Chinese Intelligence Agencies: Evolution and Empowerment in Cyberspace", in Lindsay et al., *China and Cybersecurity*, p. 32. For Mallick there are "five poisons": Tibetan separatism, Uighur separatism, Falungong activity, Taiwan's independence, and pro-democracy activism. Mallick, *China in the Cyber Domain*, p. 241.

ized executive. The exception is military intelligence. This is provided directly to the CCP.[123] Counterintelligence is a high priority for the CCP/PLA.[124]

However, because the MSS is so vast (thought the most populous of China's intelligence agencies) there is also a degree of decentralization and variation across its 31 major provincial and municipal sub-organizations. According to Mattis, these "are almost like little intelligence services and often have wide latitude to pursue sources".[125] China's broader intelligence bureaucracy is equally vast and combines a wide and expansive array of agencies, military departments, civilian policing branches, party organizations, research institutes, and media outlets.[126] These play a part in domestic "stability maintenance" (*weiwen*, 维稳), a top priority throughout China concentrated on national cohesion and for maintaining the bond between party-state (meaning the PRC is not an unqualified police state).[127]

In stark contrast to the MPS' international cooperation in investigating cybercrime (and away from their publicly declared responsibilities), members of the MSS stand accused by the FBI and U.S. Department of Justice (DOJ) of cybercrimes/cyberespionage. In 2021, four members of the MSS were indicted for running APT40 (Kryptonite Panda). APT40 has targeted a wide range of Western nations. The DOJ indicted them for targeting and exploiting companies, universities, and government agencies as part of the MSS' Hainan State Security Department through a front company (Hainan Xiandun Technology Development). The indictment alleges that the four accused MSS officers coordinated, facilitated, and managed sub-state (privateer) computer hackers and linguists at Hainan Xiandun and other MSS front companies.[128]

---

123 STRATFOR, "Intelligence Services, Part 1: Espionage with Chinese Characteristics" (March 2010), pp. 3–4.

124 Cheng, *Cyber Dragon*, pp. 113–115.

125 Peter Mattis, "Everything We Know about China's Secretive State Security Bureau" (July 9 2017), https://nationalinterest.org/feature/everything-we-know-about-chinas-secretive-state-security-21459, accessed August 21 2024.

126 STRATFOR, "Intelligence Services, Part 1: Espionage with Chinese Characteristics" (March 2010), pp. 3–4. Yuhua Wang and Carl Minzner, "The Rise of the Chinese Security State", *China Quarterly*, Vol. 222 (June 2015), pp. 339–359.

127 Wang and Minzner, "The Rise of the Chinese Security State", pp. 339–359. Xu Jinghong, "Evolving Legal Frameworks for Protecting the Right to Internet Privacy in China", in Lindsay et al., *China and Cybersecurity*, pp. 242–259.

128 "APT 40 Cyber Espionage Activities: Conspiracy to Damage Protected Computers and Commit Economic Espionage; Criminal Forfeiture", https://www.fbi.gov/wanted/cyber/apt-40-cyber-espionage-activities, accessed October 24 2021. On these naming conventions see Appendix 1: Chinese APTs.

Aside from the United States, nations targeted by APT40 included Austria, Cambodia, Canada, Germany, Indonesia, Malaysia, Norway, Saudi Arabia, South Africa, Switzerland, and the United Kingdom. Targeted sectors included government, defense, maritime aviation, education, healthcare, and biopharmaceuticals. Specifically, this encompassed confidential business information as well as intellectual property. This contained sensitive technologies for submersibles and unmanned autonomous vehicles, specialized chemical formulas, commercial aircraft servicing, and proprietary genetic-sequencing technology and data.

China's wider intelligence community aided their efforts. This was used to help secure contracts for state-owned enterprises in target states. This included large-scale high-speed railway infrastructure development projects as part of China's massive and ambitious Belt and Road Initiative (BRI) (discussed in chapter 4). In addition, infectious-disease research on Ebola, MERS, HIV/AIDS, Marburg, and tularemia (conducted in institutes and universities) was also targeted. Chinese universities were also implicated. The universities were useful in identifying hackers and linguists for potential recruitment (including fellow researchers at foreign universities). One Hainan-based university even "helped support and manage Hainan Xiandun as a front company, including through payroll, benefits and a mailing address".[129]

In March 2024, the MSS was also implicated in running APT31 (Zirconium). From around 2010 until January 2024, APT31 targeted thousands of individuals across multiple sectors in a coordinated multinational campaign. APT31 similarly operated a front company (Wuhan Xiaoruizhi Science and Technology – Wuhan XRZ) based in the suburbs of southeastern Wuhan. Their target set was wide ranging, including government officials (including some in the White House and Justice and State Departments), as well as their spouses, lawmakers, and companies across the defense-industrial base.

It also included the Inter-Parliamentary Alliance on China (IPAC), a group founded in 2020. Every European Union member of IPAC was targeted. Forty-three United Kingdom Members of Parliament, most of whom were either members of IPAC or were outspoken critics of the Chinese government, were also targeted, as were serving U.S. Senators and Representatives from both main political parties and their election staff. They also targeted the owner-operators of critical infrastructure. Individuals were targeted (including at their home addresses) for

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

access rights and intelligence gathering as well as to facilitate IP theft. Chinese political dissidents were also targeted.[130]

APT31 also targeted activists, journalists, and academics (including at the United States Naval Academy and the United States Naval War College's China Maritime Studies Institute). These cyberespionage attacks were heightened during geopolitical events affecting China. This included economic tensions with the U.S., events surrounding China's maritime claims in the South China Sea (relevant to chapter 4), and pro-democracy protests in Hong Kong in 2019 (and the crackdown that followed). Like APT40, APT31 employed a mix of Chinese state-sponsored intelligence officers, privateer contract hackers, and support staff on behalf of the Hubei State Security Department – another provincial subset of the MSS.[131]

In July 2021 then-U.S. Secretary of State Antony Blinken accused the MSS of fostering "an ecosystem of criminal contract hackers who carry out both state-sponsored activities and cybercrime for their own financial gain".[132] This was part of a policy to "name and shame" the MSS/PRC (discussed in chapter 2).[133] According to the U.S. Department of Justice indictment, this included "theft … focused on information that was of significant economic benefit to China's companies and commercial sectors, including information that would allow the circumvention of lengthy and resource-intensive research and development processes".[134]

9 Chinese cyberespionage and their tactics, techniques, and procedures

The PRC's modus operandi (known as tactics, techniques, and procedures) is common to organized cybercriminal groups (which can help obscure the actor and agency behind them). For example, APT40 used The Onion Router to increase anonymity, third parties and third-party apps (including those stored on the online de-

130 https://www.justice.gov/usao-edny/media/1345131/dl (January 30 2024), accessed August 21 2024.
131 "Treasury Sanctions China-Linked Hackers for Targeting U.S. Critical Infrastructure" (March 25 2024), https://home.treasury.gov/news/press-releases/jy2205, accessed August 21 2024.
132 Press Statement, Antony J. Blinken, Secretary of State, July 19 2021, Responding to the PRC's Destabilizing and Irresponsible Behavior in Cyberspace, https://www.state.gov/responding-to-the-prcs-destabilizing-and-irresponsible-behavior-in-cyberspace/, accessed October 16 2021.
133 Bill Gertz, "'Name and Shame' Campaign Offers Rare Glimpse into China's Cyber Operations: U.S. Indictment Targets Workings of Shadowy Ministry of State Security" (July 20 2021), https://www.washingtontimes.com/news/2021/jul/20/china-cyber-operations-exposed-name-and-shame-camp/, accessed October 16 2021.
134 https://www.justice.gov/opa/pr/four-chinese-nationals-working-ministry-state-security-charged-global-computer-intrusion (July 19 2021), accessed October 16 2021.

positories Dropbox and GitHub), and sent spear-phishing e-mails supported by fictitious online profiles. Links were often embedded to doppelgänger domain names. These "watering hole" attacks resemble the domain names of legitimate companies and mimic or duplicate their pages and are known to host malware (malicious software).[135]

Malware is in constant development and can be reengineered as well as refined. Customized malware is used alongside community-developed malware. Both are used to penetrate, expand, and maintain unauthorized access to devices and networks by cybercriminal gangs and APTs. Nation-states like China can remain undetected whilst able to maintain persistent access against countermeasures. Persistence (the P in APT) is not a prevalent feature of cybercriminal gangs. Cybercrime gangs will frequently move on to less well defended targets (the lower-hanging fruit).[136] Chinese espionage/cyberespionage can also employ steganography (concealing an image or information inside other images, information, or files).[137] Steganography is a long-standing intelligence method, and this and other tools of spycraft are used to support Chinese cyberespionage.

The linkages between cybercrime and state-supported or -sanctioned cyberespionage and the use of "false flags" to help mask attribution are becoming more evident. State-run APT campaigns, like those out of China, can be solely cyberespionage operations conducted remotely but they can also leverage traditional intelligence methods including HUMINT gathering and exploitation. Leveraging the "Money, Ideology, Compromise/Coercion, Ego" (MICE) framework, this includes Social Engineering, honey traps (creating a compromising situation for a target, often through sex), and Swallows and Romeos (agents who seduce a target for intelligence purposes).[138] This has seen Chinese intelligence agencies exploiting not only the open borders of cyberspace but also a wide spectrum of Western society in the real world (the social layer). This includes through Chinese companies and Chinese academia.[139] This will be discussed in chapter 3, which will detail clear evidence of intensifying and coordinated cyber campaigns against Western nation-

135 Stoddart, *Cyberwarfare*, pp. 31–33, 230–231. "Malware" is now the industry standard term encompassing viruses, worms, trojans, and automated bots.

136 Stoddart, *Cyberwarfare*, pp. 227–280, 355–357, 368–376, 415–418.

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

138 Scott Shumate and Randy Borum, "Psychological Support to Defense Counterintelligence Operations", *Mental Health Law & Policy Faculty Publications*, Paper 546, Vol. 18, No. 4 (January 2006), p. 291.

139 James M. Olson, *To Catch a Spy: The Art of Counterintelligence* (Washington DC: Georgetown University Press, 2021), pp. xi-xv, 1–12. "How the U.S. Caught a Chinese Spy" (CNBC), https://www.youtube.com/watch?v=0ydtETPStEI, accessed March 18 2024.

states since the early to mid-2000s allied to traditional intelligence-gathering and espionage operations. This modus operandi is another theme of this book.

10 The lawfulness of cyberespionage

There are over one hundred national intelligence agencies spread around the globe, including those mentioned above. Some states, especially democratically accountable states, have increasingly (publicly) acknowledged their own intelligence agencies (and those of other nations) but operational matters are rarely discussed. By acknowledging their agencies and countermeasures through oversight and accountability, they are tacitly or explicitly deeming their activities legitimate and essential in protecting national security. At the same time, denunciation of foreign espionage is often heard loudly and clearly.

Importantly, espionage and cyberespionage (whilst breaking national laws), including from China, are permissible under international law. Spying is rarely acknowledged whilst it is occurring, nor commented on, nor denied (even decades afterwards). According to the legal scholar Darien Pun, widespread state "engagement in espionage makes the behavior permissible" whilst "The lack of explicit historical prohibition of peacetime espionage in international law has created a customary norm for its permissibility".[140]

Foreign activities such as China's are criminalized under domestic law, and cases are prosecuted (though many are not). Cases can include domestic spying by foreign governments or double agents (who spy for a foreign government). Assets are actively recruited whilst some voluntarily offer their services (known as "walk-ins"), becoming moles. Chinese moles include Jerry Chun Shing Lee and Kevin Mallory. Both were former CIA agents bribed to spy for Chinese intelligence. CIA moles within China have also been uncovered by Chinese counterintelligence. This is discussed further in chapters 3 and 4. For Pun, this points to a double standard and "International law struggles with clarity in the face of this strange 'doublethink' tension, plagued with seemingly ideological contradictions".[141]

China has developed into a mature espionage user. The centuries-old recruitment and retention tools of MICE remain part of the toolbox and tradecraft of Chinese intelligence; as they do for many other nations and sub-state and non-state

140 Darien Pun, "Rethinking Espionage in the Modern Era", *Chicago Journal of International Law*, Vol. 18, No. 1 (Summer 2017), pp. 361–362.

141 Pun, "Rethinking Espionage in the Modern Era", p. 355.

organizations and groups (including for corporate espionage and terrorism).[142] HUMINT and traditional spycraft are now allied to the overt and covert use of cyber as part of the intelligence-gathering toolbox because, "Like many other fields, espionage is being transformed by the 'cyber' prefix or descriptor".[143]

Then-FBI Director Christopher Wray stated in July 2020 that the FBI was launching new Chinese-related counterintelligence cases around every 10 hours. Half of the FBI's 5,000 active counterintelligence investigations now relate to what has become a whole-of-nation effort by the PRC. China is employing a wide range of actors, companies, and enterprises for these efforts. This was part of what Wray termed "a generational fight" to overtake the United States.[144]

China is far from alone in conducting cyberespionage operations allied to traditional spycraft. In 2013, Edward Snowden leaked a trove of documents from his employers, the NSA. This lifted the lid on a massive and pervasive international mass data collection and analysis program involving their "Five Eyes" partners: Britain, Canada, Australia, and New Zealand. The fallout from the Snowden disclosures meant that the two-year negotiations on what became the Obama–Xi agreement, outlined in chapter 3, saw the United States lose moral high ground and hamper negotiations with China on trust building and limiting cyberespionage.[145]

Chinese hackers can also be working for industrial competitors (industrial or corporate espionage) or be hackers for hire. Hackers for hire can be freelancing but there is also evidence that "Chinese hacking groups were [are] known to pursue commercial crimes alongside their state-backed operations".[146] This includes individuals hacking "for their own personal financial gain" as well as "for the ben-

142 Peter Mattis and Matthew Brazil, *Chinese Communist Espionage: An Intelligence Primer* (Annapolis, MD: Naval Institute Press, 2019). Roger Faligot, *Chinese Spies: From Chairman Mao to Xi Jinping* (London: Hurst, 2019).

143 Pun, "Rethinking Espionage in the Modern Era", p. 355.

144 Christopher Wray, Director Federal Bureau of Investigation, Hudson Institute, Video Event: "China's Attempt to Influence U.S. Institutions", Washington, D.C. (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 March 2 2024.

145 Tang Lan, "World's Largest Internet Hacker", http://www.chinadaily.com.cn/opinion/2014-06/04/content_17560641_2.htm, accessed February 1 2019.

146 "Double Dragon APT41: A Dual Espionage and Cyber Crime Operation" (2019), https://content.fireeye.com/apt-41/rpt-apt41/. Joseph Menn, Jack Stubbs, and Christopher Bing, "Chinese Government Hackers Suspected of Moonlighting for Profit" (August 7 2019), https://www.reuters.com/article/us-china-cyber-moonlighters-idUSKCN1UX1JE. Both accessed October 9 2021. For deeper background see Zhuge Jianwei, Gu Lion, Duan Haixin, and Taylor Roberts, "Investigating the Chinese Online Underground Economy", in Lindsay et al., *China and Cybersecurity*, pp. 87–120.

efit of the MSS or other Chinese government agencies".[147] In addition, Chinese commercial companies also develop malware for government use. This was detailed in a data leak posted on GitHub in February 2024.[148] These proxies or "privateers" obscure state involvement and undermine the international Rule of Law. Outsourcing or tacitly permitting cybercriminal acts also blurs the lines between (cyber)crime and (cyber)espionage, especially when state on state, and the Rules of Engagement.

Using criminal gangs as "privateers" has long been part of Russian tactics (practices mirrored North Korea and Iran) but for China, with its tight domestic controls over Internet use (termed "the Great Firewall"), this is something new.[149] This is blurring the lines between state-sponsored hacking groups and third parties hired or contracted by the Ministry of State Security. This includes the reuse of malware variants between groups alongside parallel PLA-run operations and campaigns.[150] This intermix is not restricted to China.

It is a large and complex picture. In 2023, there were an estimated 1.09 billion Internet users ("netizens") in China (78 percent of its population). Where this lags is in remote, rural regions.[151] Some 1.2 billion use WeChat, the most popular social media platform and instant messaging app in China. It is also popular with the Chinese diaspora worldwide. Owned by the Chinese technology company Tencent, it (like many other Chinese social media platforms) has "faced the challenge of mon-

---

147 Two Chinese Hackers Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including COVID-19 Research (July 21 2020), https://www.justice.gov/opa/pr/two-chinese-hackers-working-ministry-state-security-charged-global-computer-intrusion, accessed October 9 2021.

148 Unit 42, "Data from Chinese Security Services Company i-Soon Linked to Previous Chinese APT Campaigns" (February 23 2024), https://unit42.paloaltonetworks.com/i-soon-data-leaks/, accessed March 18 2024.

149 Paul Mozur and Chris Buckley, "Spies for Hire: China's New Breed of Hackers Blends Espionage and Entrepreneurship" (August 26 2021), https://www.nytimes.com/2021/08/26/technology/china-hackers.html, accessed October 9 2021. For a deeper dive into Chinese cybercrime see Recorded Future/Insikt Group, "Illegal Activities Endure on China's Dark Web Despite Strict Internet Control" (October 5 2021), https://go.recordedfuture.com/hubfs/reports/cta-2021-1005.pdf, accessed October 10 2021.

150 Catalin Cimpanu, "Sprawling Cyber-espionage Campaign Linked to Chinese Military Unit" (June 16 2021), https://therecord.media/sprawling-cyber-espionage-campaign-linked-to-chinese-military-unit/, accessed October 10 2021.

151 "Internet Usage in China – Statistics & Facts" (last updated April 16 2024), https://www.statista.com/topics/1179/internet-usage-in-china/, "Number of Internet Users in China from 2014 to June 2024", https://www.statista.com/statistics/265140/number-of-internet-users-in-china/. Both accessed November 23 2024.

itoring and censorship by the government".[152] This also includes the platforms Sina Weibo and TikTok. There are also claims of government-sponsored groups seeking to influence public opinion through indigenous services and Western platforms including Twitter/X and Facebook/Meta (both of which are banned with VPN use restricted in China). Influencing utilizes astroturfing (a method of creating impressions of widespread support), sock puppets (authors of fake social media accounts), "content farms", and the use of bots to spread messaging.[153]

11 Traditional intelligence gathering, espionage, and cyberespionage

Various intelligence agencies around the world recruit and handle human intelligence assets, and produce intelligence gathered from HUMINT and other sources to produce all-source intelligence. China is among them. Many intelligence agencies conduct espionage and undertake covert action or active measures with international tradecraft, sharing much in common (with variations).[154] CIA historian Michael Warner describes covert action as "the various arts of subversion and sabotage".[155] Plausible deniability is a feature of covert action (comparable to Russian active measures). Warner has contemplated whether cyberespionage should be reconsidered not as a form of covert action but as covert action in itself (in actuality, tailor made for covert action). Part of Warner's reasoning is the types, scale and scalability, and deep reach of cyber operations across a spectrum of activities.[156] This book, and its two companion volumes, support Warner's hypothesis. Whilst cyberespionage requires tailored analysis, it is not all together a completely novel experience.

Espionage and spying have been around since before biblical times, often clouded in secrecy through the largely secret activities of what have become intelligence agencies. Specifically, espionage is a process through which information not publicly available is obtained. Espionage can include the recruitment and run-

152 Eric Harwit, "WeChat: Social and Political Development of China's Dominant Messaging App", *Chinese Journal of Communication*, Vol. 10, No. 3 (2017), p. 324.

153 Mallick, *China in the Cyber Domain*, pp. 257–284. Jovy Chan, "Online Astroturfing: A Problem Beyond Disinformation", *Philosophy & Social Criticism*, Vol. 50, Issue 3 (March 2024), pp. 507–528.

154 Len Scott, "Secret Intelligence, Covert Action and Clandestine Diplomacy", *Intelligence and National Security*, Vol. 19, No. 2 (Summer 2004), pp. 322–341.

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

156 Warner, "A Matter of Trust", pp. 37–40.

ning and handling of human sources (HUMINT), technical means (including hacking and cracking computer systems), and other covert activities. It can be used to attempt to influence decisionmakers and opinion formers or used to gather actionable intelligence. Classification exists to protect the intelligence agencies (especially their sources and methods), and guard national security, the economy, and state institutions. Classification is also employed to protect military operations and personnel, weapon systems, and other operational concerns. It also (increasingly) embraces civilian critical infrastructure sites and networks, and extends to protecting classified or restricted technologies.[157]

Nevertheless, one of the main themes of this book and its companion volumes is that cyberespionage has characteristics that create threatening ambiguity between intelligence gathering and offensive operations. This is novel. This is a multi-pronged approach which for China has become a whole-of-nation effort where businesses, universities, and citizens are expected to assist the government under national security laws. Much of this is geared around technology acquisition but it is adjacent to forays into critical infrastructure. This includes defense technologies. It was estimated in 2021 that the United States loses $200-$600 billion a year through the theft of research and development. This loss of IP is cumulatively estimated at between $4 trillion and $12 trillion since the end of the Cold War.[158] This loss is not only economic, and neither are the gains to the acquirer. The U.S. is not the only target, but it is the primary target. This is the subject of chapter 3. How this innovation is being used in China's defense industries, the subject of chapter 4.

Cyberattacks mainly originate from mainland China, but this book will also analyze cases where industry insiders have been targeted and where Chinese academia, companies, and business people at home and abroad are leveraged, or where Chinese intelligence is suspected of "hacking to order". Christopher Wray remarked in 2020 that Chinese cyberespionage involves state-owned enterprises as well as Chinese intelligence services. It also includes corrupting trusted insiders and physical theft, researchers, and graduate students, alongside a whole variety of other actors. This has led them to pioneer "an expansive approach" to economic and innovation espionage which increased by around 1,300 percent between 2010 and 2020.[159]

China is also known to invest in or buy out companies in sectors of strategic interest, from technology firms to pharmaceuticals and renewable energy. It also

157 Espionage, https://www.mi5.gov.uk/espionage, accessed November 1 2016.

158 "Top Counterintelligence Official Mike Orlando on Foreign Espionage Threats Facing U.S. – 'Intelligence Matters'" (May 12 2021), https://www.cbsnews.com/news/foreign-espionage-threats-u-s-intelligence-matters-podcast/, accessed March 4 2024.

159 Wray, "The Threat Posed by the Chinese Government".

targets government organizations and gathers intelligence and *kompromat* on insiders working within target organizations. Through China's "Thousand Talents Program" and related plans, Chinese working abroad are incentivized to overtly and covertly divert their research work to the PRC.[160] As well as targeting human rights organizations, Taiwan, and government critics at home and abroad, the CCP also has levers of control over companies operating in the private sector.[161] This includes large corporations like Huawei, the world's largest telecommunications equipment manufacturer. Meanwhile, foreign businesses seeking to work in China have to comply with conditions set out by the CCP for access to the "El Dorado that is the Chinese consumer base".[162] Those who enter China hoping to do business are advised to take "burner phones" with them or risk their stored contacts, e-mails, texts, and data use be subject to state surveillance.[163]

As indicated above, China also seeks to actively recruit agents from rival foreign intelligence services. This is true of many other nations but in America 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. Money (the M in MICE) is the usual dangle. Thereafter, covert communications are established, followed by tasking recruits through progressive requests, especially for restricted or classified information.[164] What this hacked data is and how it is useful is discussed in chapters 2–4. Added to this are potential "walk-ins" (those who voluntarily offer their services) or whistleblowers such as Edward Snowden.[165]

---

160 Wray, "The Threat Posed by the Chinese Government". Jeffrey Stoff, "China's Talent Programs", in William C. Hannas and Didi Kirsten Tatlow (eds.), *China's Quest for Foreign Technology: Beyond Espionage* (New York: Routledge, 2021), pp. 38–54.

161 Sarah McKune, "'Foreign Hostile Forces': The Human Rights Dimension of China's Cyber Campaigns", in Lindsay et al., *China and Cybersecurity*, pp. 260–293.

162 Andrew Soergel, "Trading Silence for Access: The Cost of Doing Business in China: The West Once Saw Trade with China as a Path to a More Open and Democratic World. Not Anymore" (October 11 2019), https://www.usnews.com/news/economy/articles/2019-10-11/trading-silence-for-access-the-cost-of-doing-business-in-china, accessed October 10 2021.

163 Liza Lin and Yoko Kubota, "Burner Phones, Bug Sweeps: How Companies Cope with IP Theft in China" (March 16 2018), https://www.wsj.com/articles/burner-phones-bug-sweeps-how-companies-cope-with-ip-theft-in-china-1521204806, accessed October 10 2021.

164 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, accessed October 10 2021.

165 James Clapper, the Director of National Intelligence at the time, remarked that because of Snowden, "We are expanding our insider-threat protection capability by monitoring the electronic behavior of employees on duty. We are in the process of transitioning the clearance process to one

When intelligence agencies (including China's) are running operatives and operations abroad, cyber brings real-time intelligence value even as it potentially increases the risk of eavesdropping, discovery, interception, and infiltration. As well as double agents like Lee and Mallory, operations usually involve two streams of operatives. Some act under diplomatic cover as official government employees holding diplomatic immunity. Official cover often includes government appointments to embassies, consulates, or intergovernmental organizations like the United Nations and its agencies. This sometimes mitigates the inherent risks of clandestine intelligence gathering.

Others, sometimes termed "illegals", operate under non-official cover (NOC). NOC can vary. It can be provided by legitimate professions including businesses, accredited media outlets, or affiliations with academia. These can involve false as well as genuine identities. The Chinese expatriate community are actively leveraged. This includes legitimate academics and business people operating as surrogates or proxies at the request of the Chinese government. It has also included alleged political employees abroad.[166] NOC operations are believed to be run from the First Bureau of the MSS. The Second Bureau is said to run overseas collection via legal residencies (such as embassies and consulates).[167] More broadly, peacetime and wartime espionage have "received different treatments".[168] That line is now blurring because whilst espionage can act as a warning indicator, peacetime cyberespionage is (amongst other things) aiding pre-positioning in critical infrastructure.[169] This is the subject of chapter 2.

12 Cyberwarfare through pre-positioning in CI

CI includes public utilities such as electric power generation and distribution, water supplies and treatment, natural gas and oil production and pipelines, shipping and maritime traffic handling, hydroelectric dams, traffic lights, and train

---

of continuous evaluation … Our system is based on personal trust. When it comes down to it, that is what it's all about." Loch K. Johnson, "A Conversation with James R. Clapper, Jr., the Director of National Intelligence in the United States", *Intelligence and National Security*, Vol. 30, Issue 1 (January 2015), p. 17.

166 Press Release: Former High-Ranking New York State Government Employee Charged with Acting as an Undisclosed Agent of the People's Republic of China and the Chinese Communist Party (September 3 2024), https://www.justice.gov/usao-edny/pr/former-high-ranking-new-york-state-government-employee-charged-acting-undisclosed, accessed September 4 2024.

167 Inkster, "The Chinese Intelligence Agencies", p. 32.

168 Pun, "Rethinking Espionage in the Modern Era", p. 360.

169 Stoddart, *Cyberwarfare*, introduction and chapter 1, pp. 1–146.

switching systems. These are the backbones of a modern developed state. Cyberespionage into these sectors gives it offensive characteristics which can be misperceived or augment fears of impending attack, either as standalone events, such as a widespread or sustained power cut, or used during a crisis. This complicates its uses and deducing "when an armed attack might occur, and in order to repel an armed attack, the capabilities of potentially hostile states".[170]

Espionage and cyberespionage are still only part of the picture. At the far end of the cybersecurity spectrum is the potential to degrade, disrupt, and damage societies and nations by regional or national attacks upon CI. CI is dependent upon Supervisory Control and Data Acquisition (SCADA) systems. Part of a wider technology layer of Industrial Control Systems (ICS), SCADA enables the management of and remote access for control and monitoring devices and processes. This includes field devices in dispersed locations. SCADA and ICS are the underlying control systems "for most critical infrastructure including power, energy, water, transportation, [and] telecommunication" as well as pipelines, manufacturing factories, and localized climate control.[171] Cyber-kinetic attacks upon CI have, so far, been limited to:

- the Stuxnet worm (discovered in 2010) that infiltrated Iran's Natanz nuclear enrichment plant (where it span uranium-enriching centrifuges beyond their limits);
- Iran's Shamoon wiperware (which deleted data), used against Saudi Aramco in Saudi Arabia in 2012;
- a steel mill in Germany in 2014 (causing massive damage);
- Russian attacks on Ukraine's power grid (where it forced power stations offline) in 2015/16.[172]

These proof-of-concept attacks notwithstanding, cyberespionage activities against CI targets are highly active, highly invasive, and deeply worrisome. The reasons behind cyberattacks on CI remain multifarious, but Verizon's 2019 Data Breach Inves-

170 Pun, "Rethinking Espionage in the Modern Era", p. 375.

171 Bonnie Zhu, Anthony Joseph, and Shankar Sastry, "A Taxonomy of Cyber Attacks on SCADA Systems", 2011 IEEE International Conferences on Internet of Things, and Cyber, Physical and Social Computing, p. 380, https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6142258, accessed July 21 2019. SCADA and ICS form a significant part of CI and are described in detail in Stoddart, *Cyberwarfare*, esp. pp. 1–52.

172 Stoddart, *Cyberwarfare*, pp. 73–79, 86, 112–113, 150–155, 161–163, 168, 194–195, 202–203. Robert M. Lee, Michael J. Assante, and Tim Conway (SANS/ICS), "ICS CP/PE (Cyber-to-Physical or Process Effects) Case Study Paper – German Steel Mill Cyber Attack" (December 14 2014), https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/bltc79a41dbf7d1441e/607f235775873e466bcc539c/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf, accessed March 8 2024.

tigations Report listed among them the long-standing problem posed by espionage.[173] This encompasses espionage from states as well as private companies (corporate espionage). Chinese intelligence has made significant inroads through this alignment.

Intrusions and breaches into CI in America, the West more widely, many of China's near neighbors in Asia and the Asia-Pacific, and to nations engaging with China's BRI, are constantly reported. This is largely a dormant threat but holding critical infrastructure "at risk" places China in a strategically advantageous position and in a powerful negotiating position. The ability to keep CI "at risk" also has the capacity to degrade and disrupt military responses to Chinese territorial and economic ambitions and advancement. Globally, increasing dependency on ICT and its backbone architecture, combined with security flaws in hardware and software, has simultaneously increased our vulnerability to cyberattack which includes the potential for cyberwar through attacks on CI.[174] In his opening address to a House Select Committee in January 2024, Chrisopher Wray warned:

> There has been far too little public focus on the fact that PRC hackers are targeting our critical infrastructure – our water treatment plants, our electrical grid, our oil and natural gas pipelines, our transportation systems – and the risk that poses to every American requires our attention now … If or when China decides the time has come to strike, they're not focused solely on political or military targets. We can see from where they position themselves, across civilian infrastructure … [these] low blows aren't just a possibility in the event of a conflict … the PRC's cyber onslaught goes way beyond [into] prepositioning for future conflict.[175]

13 9/11: Counterterrorism priorities but increasing state threats

There are multiple, systemic reasons for this insufficient focus. Underlying reasons include the evolution of the Internet and growing hyperconnectivity, legacy systems, malware development, an ever-widening attack surface, and the multiplicity

173 "2019 Verizon Data Breach Investigations Report", pp. 8, 18, https://www.fbcinc.com/e/docitcyber/presentations/Verizon2019DataBreakInvestigationsReport.pdf, accessed April 6 2020.

174 There are competing and contested views of what "cyberwar" means. This was the subject of chapter 2 of Stoddart, *Cyberwarfare*, pp. 53–114. In the Chinese context see also Lindsay, "China and Cybersecurity: Controversy and Context", pp. 5–6 as well as Jason R. Fritz, *China's Cyber Warfare: The Evolution of Strategic Doctrine* (Lanham, MD: Lexington Books, 2017).

175 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.

of threat actors. Much of this was systematically analyzed in *Cyberwarfare: Threats to Critical Infrastructure.*[176] In addition, there has been an inadequate focus on Chinese cyberespionage because of changes in the geopolitical threat landscape.

Following the end of the Cold War, in the two decades from 1991–2011, new questions were asked of Western intelligence services which for so long had been geared towards the perceived threat from the Soviet Union and its communist allies more generally. Then-CIA Director, R. James Woolsey stated at his Senate confirmation hearing in 1993, "We have slain a large dragon. But we now live in a jungle with a bewildering variety of poisonous snakes. And, in many ways, the dragon was easier to keep track of."[177] This dragon slaying stripped the U.S. (and wider Western) Intelligence Community of much of their *raison d'être* (particularly the CIA).

The PRC was still a rising power in 1991 and in 1989 had faced a popular uprising culminating in the Tiananmen Square protests. The PRC was not the politico-military and economic power it is today and its erstwhile communist ally, the USSR, had collapsed along with the Warsaw Pact and Eastern European communism. This was, as Francis Fukuyama contended, *The End of History*.[178] The IC in the U.S. and wider Western world might have been slow in turning towards this (and other) systemic changes. The policy community is mission driven and its priorities, missions, and targets are assigned to them. The IC is obligated to respond. These are politico-militarily directed and whilst missions may be enduring, their form and function can change.

The enduring missions include collection and analysis on "hard target" countries such as China, Cuba, Iran, North Korea, and Russia, as well as a plethora of other threats and dangers. These include long-standing issues of chemical, biological, and nuclear weapons proliferation. It also includes economic security, environmental concerns, organized crime, terrorism, and other transnational threats.

---

176 Stoddart, *Cyberwarfare*, pp. 1–35, 147–424.

177 Quoted in Michael J. Sulick, *American Spies: Espionage against the United States from the Cold War to the Present* (Washington DC: Georgetown University Press, 2013), p. 183.

178 Samuel Huntingdon also contended this foreshadowed a clash of civilizations. Francis Fukuyama, "The End of History", *The National Interest*, No. 16 (Summer 1989), pp. 3–18. Francis Fukuyama, *The End of History and the Last Man* (New York: Free Press, 1992). 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). Both Fukuyama and Huntingdon have reassessed and revised their original theses, and they remain subjects of active debate. Francis Fukuyama, "The 'End of History' 20 Years Later", *New Perspectives Quarterly*, Vol. 27, Issue 1 (Winter 2010), pp. 7–10. Samuel P. Huntingdon, "The Clash of Civilizations Revisited", *New Perspectives Quarterly*, Vol. 30, Issue 4 (October 2013), pp. 46–54.

During the mid-1990s, the priority for the USIC was in protecting and supporting warfighters engaged in overseas combat and humanitarian operations. This included United Nations-mandated peacekeeping missions in former Yugoslavia, Somalia, and Haiti. As a result "the Intelligence Community was faced not with the absence of a mission, but arguably an excess of them … but establishing these priorities is a political decision".[179] These priorities can change in response to new threats.

On September 11 2001 a new (or gravely changed) threat emerged. Al-Qaeda attacked the Twin Towers of the World Trade Center in New York and the Pentagon, home of the Department of Defense, in Arlington, Virginia. A fourth attack on Washington D.C. aimed at either the Capitol Building or White House was only prevented by the brave actions of the passengers aboard United Airlines Flight 93. The devastating terrorist attacks of 9/11 led directly to the decision to invade and then occupy Afghanistan, the main location of Al-Qaeda.[180] It took a further decade for Osama Bin Laden, the head of Al-Qaeda and mastermind of 9/11, to be located and killed by U.S. Special Operations Forces in Abbottabad, Pakistan in May 2011.[181] It took a decade more for U.S.-led coalition forces to exit Afghanistan in Autumn 2021 (to much discord), leading to a swift return to the repressive rule of the previously deposed Taliban.[182]

In the interim, Iraq had been invaded in 2003 under a UN mandate based on false intelligence assessments of Iraqi WMD programs. That mission ended in 2011, with the final U.S. presence leaving in 2021. An in-area presence remained. Both occupations were central to the "War on Terror".[183] Whether "mission accomplished" has been achieved through intervention and democracy promotion spanning the George W. Bush, Obama, Trump, and Biden administrations, is questionable.[184]

---

179 William C. Prillaman and Michael P. Dempsey, "Mything the Point: What's Wrong with the Conventional Wisdom about the C.I.A", *Intelligence and National Security*, Vol. 19, No. 1 (Spring 2004), p. 6.

180 "The 9/11 Commission Report", pp. 14, 45, 155, 166, 243–244, 248, 326, https://www.9-11commission.gov/report/911Report.pdf, accessed January 13 2019.

181 Christian Schaller, "Using Force Against Terrorists 'Outside Areas of Active Hostilities' – The Obama Approach and the Bin Laden Raid Revisited", *Journal of Conflict and Security Law*, Vol. 20, Issue 2 (Summer 2015), pp. 195–227.

182 Phil Williams, "US Intervention in Afghanistan and the Failure of Governance", *Small Wars & Insurgencies*, Vol. 33, Issue 7 (2022), pp. 1130–1151. Robert S. Snyder, "The Fall of Afghanistan: An American Tragedy", *Small Wars & Insurgencies*, Vol. 34, Issue 4 (2022), pp. 747–758. Toby Dodge, "Afghanistan and the Failure of Liberal Peacebuilding", *Survival*, Vol. 63, Issue 5 (September 2021), pp. 47–58.

183 Later the "Global War on Terror" (GWOT).

184 Hal Brands, "Blundering into Baghdad: The Right – and Wrong – Lessons of the Iraq War", *Foreign Affairs*, Vol. 102, No. 2 (March/April 2023), pp. 176–184.

A series of popular uprisings known as the "Arab Spring", which began in earnest in 2011, soon spread across the Middle East and North Africa (MENA). The withdrawal from Iraq was a contributory factor. It also contributed to the chaos that engulfed the MENA, especially Iraq and Syria, in the wake of the Arab Spring leading to the rise of the so-called Islamic State whose "Caliphate" brutally occupied areas of Iraq and Syria between 2014 and 2019/20.[185] Many parts of the MENA remain unstable still and on October 7 2023 the Hamas–Israel conflict ignited once more in the Middle East.[186] In December 2024, the Assad regime fell in Syria.

America and its allies and friends not only continue to face an excess of threats and threat actors from states and non- and sub-state actors, but for over two decades since 2004 the underbelly of the U.S. and Western society and its economic foundations have also been attacked. This occurred whilst reorienting from the change in intelligence and foreign policy focus after 9/11 which saw counterterrorism accorded a higher priority under the spotlight of a perceived intelligence failure.[187] The extent to which this led to systemic decline in specialist Sinology (and "Sovietology") in the USIC is also pertinent. It, too, is a theme of this book and the companion books on Russia and Cyberwarfare.

9/11 had other implications, too. The 9/11 Commission discovered that the intelligence needed to prevent the attacks was contained in the USIC bureaucracy but was disassembled in a sea of information. This led to reforms which have promoted greater intelligence sharing. This seemingly prioritized the need-to-share above need-to-know concerns. This also carries risks. As a result, undetected U.S. insiders with top secret access, including Edward Snowden, Bradley Manning, and Jack Teixeira, have leaked secrets.[188] That security vetting and monitoring procedures did not discover them in advance are also intelligence failures.

---

185 Imad Salamey, "Post-Arab Spring: Changes and Challenges", *Third World Quarterly*, Vol. 36, No. 1 (January 2015), pp. 125–126. Hassanein Ali, "The Rise and Fall of Islamic State: Current Challenges and Future Prospects", *Asian Affairs*, Vol. 51, Issue 1 (January 2020), pp. 71–94.

186 Zohar Lederman, Nadav Davidovitch, and Shmuel Lederman, "Making a Case for Appropriate and Humane Treatment of Hamas Belligerents in Israel", *American Journal of Bioethics*, Vol. 24, Issue 2 (February 2024), pp. 8–10.

187 "The 9/11 Commission Report", p. 336. The Commission pointed to a "failure of imagination" in preventing 9/11 as a result of deficient foresight and the benefit of hindsight (pp. 339–360).

188 Helene Cooper and Eric Schmidt, "Ukraine War Plans Leak Prompts Pentagon Investigation: Classified Documents Detailing Secret American and NATO Plans have Appeared on Twitter and Telegram" (April 6 2023), https://www.nytimes.com/2023/04/06/us/politics/ukraine-war-plan-russia.html. Emma L. Briant, "How Social Media Incentives Helped Drive the Discord Leaks" (May 1 2023), https://techpolicy.press/how-social-media-incentives-helped-drive-the-discord-leaks/. Both accessed July 10 2023. Former Air National Guardsman Sentenced to 15 Years in Prison for Unlawfully Disclosing Classified National Defense Information (November 12 2024), https://www.justice.gov/opa/

Increasing the numbers eligible for clearance increases espionage risks. The number of personnel eligible for clearance in the U.S. was over 4 million people in 2017 (the last publicly available figure). Of these, 390,000 had been granted confidential/secret clearance, with a further 206,000 granted top secret clearance.[189] Adding to the uncertainty, the U.S. Government Auditing Office also reported a lack of interagency trust in respect to security clearance processes.[190] Given this, and the cases of Snowden, Manning, and Teixeira, it is concerning that Scattered Castles, the database used by the USIC to administer security clearances, might itself have been the subject of a Chinese cyberespionage campaign as part of the breach of the Office of Personnel Management between 2013 and 2015 (discussed in chapter 4).

Over 20 years on from 9/11, increasingly networking has also increased the volume of information-intelligence by orders of magnitude. This further alters intelligence gathering, operations, and processing as well as increasing the attack surface and avenues of attack.[191] China (alongside Russia) has learned to exploit these growing interconnections. How information is sifted for intelligence, how information overload is managed, and establishing better ways to find future needles in the haystack after 9/11 are an ongoing series of processes. Whilst improving intelligence sharing, intelligence analysis, and judgments might be proving effective in combating counterterrorism, it also provides windows of opportunity for China and Russia. Greater intelligence sharing might not be a panacea for intelligence failures.

All the while China has been planning and acting. Russia too. In 2014 it annexed Crimea and for eight years Russia conducted hybrid warfare against Ukraine until a decision was made to conduct a full-scale invasion by President Vladimir Putin in February 2022. That decision was partially influenced by inadequate pushback in 2014 in the form of limited sanctions and diplomatic condemnation over Crimea. It might also have been influenced by the further lack of pushback for Russia's political influence and election interference cyberespionage/active

pr/former-air-national-guardsman-sentenced-15-years-prison-unlawfully-disclosing-classified, accessed November 13 2024.

189 "Fiscal Year 2017: Annual Report on Security Clearance Determinations", p. 5, https://www.dni.gov/files/NCSC/documents/features/20180827-security-clearance-determinations.pdf, accessed March 7 2024.

190 "Actions Needed to Improve the Transfer of Personnel Security Clearances and Other Vetting Determinations" (January 2024), https://www.gao.gov/assets/d24105669.pdf, accessed March 7 2024.

191 Avi Tal and David Siman-Tov, 'HUMINT in the Cybernetic Era: Gaming in Two Worlds", *Military and Strategic Affairs*, Vol. 7, No. 3 (2015), p. 95.

measures campaigns against at least 27 Western democracies since 2004, culminating in the U.S. presidential election of 2016.[192]

So far, China's use of cyberespionage against U.S. computer systems and networks has primarily been for intellectual property theft, where Russia has seen IP theft or economic gain as a side benefit. As the U.S. National Counterintelligence Strategy for 2020–2022 detailed:

> Many countries target the United States because it is a global center for high-technology research, technology and innovation. Foreign intelligence entities have embedded themselves into U.S. national labs, academic institutions, and industries that form America's national innovation base. They have done this to acquire information and technology that is critical to the growth and vitality of the U.S. economy. Adversaries use front companies, joint ventures, mergers and acquisitions, foreign direct investment, and talent recruitment programs to gain access to and exploit U.S. technology and intellectual property.[193]

China (as well as Russia) has also conducted APT cyberespionage campaigns on critical infrastructure. There are many other state-based actors lined up against America and the West more generally, including Iran and North Korea, but they present a much lower level of threat. Rob Joyce, when a Senior Advisor in cybersecurity strategy at the NSA, analogized "Russia is the hurricane: It comes in fast and hard, China is climate change: long, slow, pervasive."[194] This book details how and why China is leveraging these climatic conditions for economic and military development and how the influence and interests of the PRC also stretch to many other parts of the globe.

14 Structure

This book begins not with China's cyberespionage campaigns but with the theories and stratagems that underpin them and have enabled the PRC to move from theo-

---

192 "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. 65–97, 99–139, https://www.foreign.senate.gov/imo/media/doc/FinalRR.pdf, accessed November 5 2019.

193 "National Counterintelligence Strategy of the United States of America 2020–2022", p. 8, https://www.dni.gov/files/NCSC/documents/features/20200205-National_CI_Strategy_2020_2022.pdf, accessed September 2 2021.

194 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, accessed October 10 2021.

ry to practice. It then moves forward to discuss what some of the results have been to date. These theories and stratagems were formed over a nearly 15-year period from 1991 through to around 2015. They undoubtedly continue to evolve as PRC capacity and capabilities advance. These are not only stratagems on cyberespionage but also contain stratagems for cyberwarfare.

Chinese theorizing of cyberespionage and cyberwarfare is dissected in chapter 1, "Decoding the dragon: Chinese theories of cyberespionage and cyberwarfare". How it has mobilized these theories into practice is analyzed in chapters 2 and 3. Chapter 1 takes a longitudinal view from lessons learned from the 1991 Gulf War through to the present. It also examines why it is pre-positioning in Western critical infrastructure. It then discusses China's use of (and cooperative agreements with) Western universities and how these are being used to enhance Chinese development and boost the private sector driven by national strategic goals. It concludes by highlighting Sino-Russian cooperation on technology transfers and exchanges on the use of cyberespionage. Like Russia, cyber has allowed China to maximize the use of the "gray zone" between peaceful competition, cooperation, and conflict.

Chapter 2, "China: critical infrastructure pre-positioning and holding it 'at risk'", looks at how China has used these theories to mobilize against CI, what Western responses have been, and the role of Chinese companies. However, chapter 2 also discusses whether the West has also pre-positioned in China's critical infrastructure and targeted high-value actors in the political, economic, military, and scientific fields, and whether this amounts to a double standard, and how it might, at least for now, be promoting deterrence. It concludes with an assessment of China's own vulnerabilities and its capacity to respond through crisis management.

Chapter 3 moves on to discuss Chinese intellectual property theft. Termed "the greatest transfer of wealth in history", it questions whether the Chinese government hacks to order for the private sector and analyzes the nature, structure, and scale of Chinese cyberespionage.[195] It also examines China's ongoing use of traditional espionage and how the shift in intelligence priorities towards counterterrorism after 9/11 has been an enabler of Chinese cyberespionage. It looks in detail at Chinese hacking campaigns across the defense-industrial base whilst questioning the value of the Obama–Xi agreement which attempted to limit Chinese cyberespionage alongside "naming and shaming" members of the PLA and other ministries. Chinese use of sub-state proxy actors is also discussed. The chapter com-

195 Keith Alexander, "Cybersecurity and American Power: Addressing New Threats to America's Economy and Military", Washington, D.C. (July 9 2012), http://www.aei.org/events/2012/07/09/cybersecurity-and-american-power/, accessed January 24 2019.

plements and builds on previous excellent work focusing on Chinese cyberespionage.[196]

What China has done with this stolen IP and how this has helped fuel China's rise (including through the massive Belt and Road Initiative) is the subject of chapter 4, "IP Theft, Military Modernization and China's Rise". This analyzes how cyberespionage acts as an enabler for Chinese development and nascent system of "alliances" through the BRI. It then moves on to discuss and detail how IP theft from the U.S. (as well as other Western powers) has been used to develop Chinese military systems. These developments, circumventing years of Western innovation and research, are enabling the PLA to project hard military power across the domains of land, sea, air, and space. The chapter then discusses whether China and America are caught in "Thucydides' Trap" and are destined for conflict, and the nature and direction of China's military, its use of "gunboat diplomacy", and possible future targets.

The conclusion will demonstrate how China's cyber campaigns damage the West but fall in the "gray zone" between peace and war. The CPC and its state organs, like their Western counterparts, are well organized and well resourced but have their own goals, national policies, and different targets. China has active and aggressive players in cyberspace and the PRC has more to gain than lose. They have helped China become a great power and one that could, or is already, rivaling the United States. It was already a rising power as the Cold War ended in the late 1980s and early 1990s. Since then, Chinese power and influence have grown. China's rise has been aided and abetted by its embrace of cyber. This has allowed China to begin to match America and the West. The end of history did not begin with the end of the Cold War, and this might be China's century. First China learned from the West and then drew its plans against us.

---

196 William C. Hannas, James Mulvenon, and Anna B. Puglisi, *Chinese Industrial Espionage: Technology Acquisition and Military Modernisation* (Abingdon: Routledge, 2013). Hannas and Tatlow (eds.), *China's Quest for Foreign Technology.* Lindsay et al. (eds.), *China and Cybersecurity.* Cheng, *Cyber Dragon.* Tai Ming Cheung, *Fortifying China: The Struggle to Build a Modern Defense Economy* (Ithaca, NY: Cornell University Press, 2009). Tai Ming Cheung, *China's Emergence as a Defense Technological Power* (Abingdon: Routledge, 2012). Tai Ming Cheung (ed.), *Forging China's Military Might: A New Framework for Assessing Innovation* (Baltimore, MD: Johns Hopkins University Press, 2014). Tai Ming Cheung and Thomas G. Mahnken (eds.), *The Gathering Pacific Storm: Emerging US–China Strategic Competition in Defense Technological and Industrial Development* (Amherst, NY: Cambria Press, 2018). Mallick, *China in the Cyber Domain.*