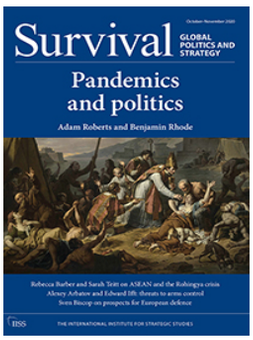

Routledge
Taylor & Francis Group

Survival
Global Politics and Strategy

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/tsur20

The Strategic Implications of China's Weak Cyber Defences

Greg Austin

To cite this article: Greg Austin (2020) The Strategic Implications of China's Weak Cyber Defences, Survival, 62:5, 119-138, DOI: 10.1080/00396338.2020.1819648

To link to this article: https://doi.org/10.1080/00396338.2020.1819648

Published online: 23 Sep 2020.

The Strategic Implications of China's Weak Cyber Defences

Greg Austin

China has raced ahead in quantum-communication technology, with remarkable achievements in teleportation of the electronic properties of remote subatomic particles.[1] In 2015, it had its first mainland-resident Nobel Prize winner in a scientific discipline (medicine).[2] Yet the innovation picture for the country is a mixed one. China publicly promotes the indigenisation of advanced technologies, including cyber capabilities, but more candid assessments do not bear out its technological nationalism. In particular, the country's leaders consider its cyber defences weak, as reflected in its continued reliance on US-based corporations for basic, front-line cyber security.[3] In 2016, for instance, President Xi Jinping complained that foreign corporations controlled China's core technologies.[4] In 2019, the Bank of China – China's leading international bank – and IBM announced a partnership in developing new cyber architectures for the bank, which has offices around the world.[5]

Western assessments confirm the weakness of China's cyber defences, although mostly in passing. The IISS's *Asia-Pacific Regional Security Assessment 2019* concluded that the country 'continues to encounter a range of challenges and potential vulnerabilities in this new domain, including the relative insecurity of its own information-technology ecosystem'.[6] US sources, often prone to exaggerating China's strengths, have begun to recognise the weaknesses in China's cyber defences.[7] According to the International Telecommunications Union's most recent cyber-security index, China ranks 27th in the world

Greg Austin is IISS Senior Fellow for Cyber, Space and Future Conflict.

Survival | vol. 62 no. 5 | October–November 2020 | pp. 119–138 DOI 10.1080/00396338.2020.1819648

This article was originally published with errors, which have now been corrected in the online version. Please see Correction (http://dx.doi.org/10.1080/00396338.2020.1833553)

in overall cyber capability, behind countries such as Croatia, Denmark, Egypt, Germany, Italy, Russia and Turkey.[8] China and Turkey have among the highest rates of malware infections. An industry website, Comparitech, has ranked China 23rd out of 76 countries based on 2019 data.[9] The World Economic Forum's 'Global Information Technology Report' ranked China 59th in network readiness in the several years up to 2016, when it was discontinued.[10] The Global Innovation Index (GII) for 2019, compiled by a consortium of reputable international organisations and not confined to cyber, ranks China 14th. China has not been in the top ten in any year since the GII was established, that range being dominated by the US and its allies.[11]

According to a report from China's National Internet Emergency Response Center in 2018, phishing cases in China decreased by 72.5% from 2016 to 2017. The number of active control terminals launching distributed denial-of-service (DDoS) attacks decreased by 46%, and the number of controlled sources launching DDoS attacks decreased by 37%.[12] But although the proportion of backdoors installed in Chinese websites decreased significantly, the volume of webpage-tampering incidents increased by 20% across all sectors, and by 30% for government websites. The annual growth rate of the number of new security vulnerabilities discovered exceeded 20%. DDoS attacks against China became more powerful, with the number of high-volume attacks (exceeding one terabyte per second) reaching 68 in 2018. The number of malicious sniffing and cyber attacks on industrial facilities, systems and platforms increased significantly. The National Internet Emergency Response Center also reported that the top three foreign sources for malicious software in China in 2018 were Canada, Russia and the United States, and that the three top ones for hosting control servers distributing this software were Germany, Japan and the US.

Leadership perceptions

In 2013, two public events demonstrated to the Chinese leadership how weak their cyber defences had been. In February of that year, the private US company Mandiant (since subsumed by FireEye) was able to penetrate one of the People's Liberation Army's (PLA) most secretive cyber-espionage teams, Unit 61398, reportedly even acquiring video footage of activity inside its

operations centre. The company publicly documented its success, which was amplified by *New York Times* reporter David Sanger in his 2018 book *The Perfect Weapon*.[13] Mandiant's infiltration revealed significant Chinese vulnerability.

In June 2013, Edward Snowden revealed widespread successful penetration of Chinese systems by the National Security Agency (NSA). Snowden claimed that the NSA had been hacking the majority of Chinese government and private systems since 2007, relying on routers provided by the US firm Cisco Systems.[14] American agencies also had been closely tracking supposedly secret cyber operations by China for several years.[15] In his State of the Union address in February 2013, president Barack Obama suggested that the US had substantial knowledge of China's cyber-intelligence operations, stating that 'our enemies are also seeking the ability to sabotage our power grid, our financial institutions, our air traffic control systems'.[16]

Chinese leaders were concerned about the security of their own high-level communications. In 2012, when Xi Jinping was assuming leadership of the country, two Western news outlets revealed explosive details of the personal wealth of the families of Xi and outgoing premier Wen Jiabao.[17] Most likely, hacks into Chinese systems produced some of the information. By 2013, electronic documents from two tax havens (the Cook Islands and the British Virgin Islands), almost certainly leaked by a Western intelligence agency,[18] led to publication of a thorough investigative report on corrupt Chinese offshore investments by the International Consortium of Investigative Journalists.[19] Intensifying leadership concerns was the constant flow of secret Chinese Communist Party documents about censorship and public security into the hands of Western analysts.[20]

To Chinese leaders, they and China's security sector seemed almost defenceless in cyberspace. The public response came in February 2014 when Xi announced his country's intent to become a cyber power and set in motion a raft of institutional reforms.[21] He explicitly linked cyber defence to national security, noting that there can be no national security without cyber security.[22] His government saw cyberspace defence as the front line of international security, reflected in a statement in China's Military Strategy 2015 that 'outer space and cyberspace have become the new commanding heights in strategic competition among all parties'.[23]

Foundations of China's national cyber security

China still has only a modest domestic cyber-security industry, a fraction of the size of its American counterpart. According to a recent report by an authoritative industry alliance, the 'overall scale of the industry is still small', around RMB39 billion (about $6bn) in 2018.[24] (The estimate does not appear to include two state-owned corporations included in the Global Fortune 500 that have cyber-security divisions.) The report notes rapid growth in the sector in recent years (18% from 2017 to 2018, and a projected annual growth rate of 20% to the end of 2021). The sector should reach RMB66.8bn ($10bn) by 2021. For comparison, in 2018 the security-related income of IBM alone, the leading US cyber-security company, grew by 55%, and revenues may have reached $4bn.[25] The report indicates that in China the 'proportion of investment allocated to cyber security within informatisation projects is still low, demonstrating an evident gap with the more developed countries in Europe and the United States'.[26]

A recent report from Tencent Security Response Centre – part of the Chinese company Tencent, one of the world's largest internet firms – offered additional explanations for the weak position of the country's cyber-security sector.[27] These included a focus on profit instead of security; high cost; a general lack of talent; concentration of the sector in Tier 1 and Tier 2 cities such as Beijing, Guangdong and Shanghai; poor cyber-security-threat technology; reliance on foreign imports for basic information infrastructure; lack of national control in core technologies; weak capability to track hostile activity (especially advanced persistent threats); reliance on out-of-date methods of protecting data; limited legal foundations for countering and tracking illegal access of data; and underdeveloped identity-authentication systems. The report observed that Chinese firms' cyber-security investment as a share of total investment (1.78%) was far lower than that in the US (4.78%) and the rest of the world (3.75%).[28]

Although China's cyber-security companies' global footprint is improving, it remains underdeveloped. Consequently, they do not benefit from internationalisation in the same way as firms such as NortonLifeLock, IBM and even Kaspersky have done. More broadly, the Chinese government has not been able to elevate its educational system to meet the cyber-power

ambition set in 2014.[29] The workforce deficit is massive. One Chinese corporation recently noted that 'the current supply of cyber security talent is approximately 100,000 while demand is expected to reach 1.4 million in 2020'.[30] Further distorting the labour market, less developed areas of China 'suffer from a lack of educational resources, hence causing poor cybersecurity practices and awareness in those regions'.[31] The massive over-concentration of trained people in a small number of cities makes the problem even worse.

The quality of cyber-security education has caught the government's attention. It has launched a number of initiatives to remedy the problem, but not on a scale that matches the shortfall in numbers or quality. For example, in its annual ranking of the country's educational institutions by discipline, the Chinese Universities Alumni Association includes none of China's universities at world-class level (nine stars) or the next level (eight stars).[32] Only two universities are graded at seven stars. By 2019, China was able to report a 16% increase in enrolments in its five undergraduate cyber-security degrees compared with the previous year, though the total numbers (fewer than 10,000) were still small relative to the need. Enrolment growth in master's degrees from 2017 to 2018 was more impressive, at 44% for a total of just over 30,000. The years between 2014 and 2018, since China declared its cyber-power ambition, had not seen such impressive growth.[33]

According to Li Aidong, deputy director-general of the Cyber Security Coordination Bureau of the Cyberspace Administration of China, the country's use of 5G 'introduces new security risks, making it possible for the network to be more infiltrated and attacked'.[34] These risks will be tougher for a country like China to handle, given its poorly developed talent pool, than for a country like the United States.

As indicated in Table 1, Western corporations (the so-called 'US alliance') hold by far the most 5G security patents, with the US company Qualcomm in the lead. It is worth noting that overall there is a surprisingly low number of patents dealing with 5G security. There will probably be more inherent security vulnerabilities in 5G technology than any intentionally created by the Chinese intelligence services, and there is no solid evidence in the public domain of gaps created specifically for Chinese spying purposes. They arise more from the nature of the technology than from the malign intent of the

Table 1: **Number of European Patent Office patents mentioning '5G' and 'security'**

Total patents mentioning '5G' and 'security'	**29,934**
Mentioning Qualcomm	2,066
Mentioning Huawei	1,387
Mentioning AT&T	1,233
Mentioning Ericsson	694
Mentioning ZTE	223

Source: European Patent Office, as of December 2019.

corporation designing the software and firmware. If Huawei's participation in national 5G networks creates vulnerabilities for Western cyber security, China itself would face reciprocal vulnerabilities that are probably more daunting: leading Western intelligence agencies can exploit Huawei technology at least as easily as Chinese agencies can.[35]

Cyber-defence weaknesses in the civil domain carry over to the military sector to a considerable degree. All countries' militaries depend in part on non-military organisations to provide cyber defences for military forces and national security. For instance, the US Department of Defense has a large civilian cyber-security workforce drawn largely from educational and training institutes in the civilian sector. So it is in China. While the country has made impressive breakthroughs in niche areas, such as quantum communications, these do not depend as much on distributed capabilities and mass interventions as cyber defence does. The cyber-defence task for the PLA is gargantuan, involving the personal security habits of hundreds of thousands of uniformed personnel as well as a large number of civilian employees and external contractors supporting PLA systems.[36]

The PLA has several major professional military-education institutions at university level that produce graduates in cyber-defence areas. The most important one now is the PLA Information Engineering University (IEU) in Zhengzhou, subordinate to the Strategic Support Force. This university is the only officially designated national cyber-security personnel-training base for the PLA.[37] It has more than 2,000 teaching and research staff, including 153 doctoral supervisors and 447 master's supervisors. The overall size of the IEU disguises its intense concentration of resources in teaching cyber defence. It takes a multidisciplinary approach that integrates

Table 2: **Number of planned IEU places by major for 2013, 2018 and 2019**

Major	2013	2018	2019
Communications engineering (communications techniques and application)	30	10	17
Communications engineering (communications-equipment research and protection)		10	14
Information engineering (signal analysis and treatment)	25	40	30
Artificial intelligence (treatment of artificial-intelligence data, research and development of equipment)	0	0	30
Information-confrontation techniques (cyber defence and attack)	0	20	20
Information security (cyber defence and attack)	89	24	20
Information security (information management)		0	64
Electronic science and technology (information-equipment techniques and protection)	0	35	20
Management science and engineering (information management)	0	30	85
Confidentiality management	0	0	85
Microelectronics science and engineering (information-equipment techniques and protection)	0	20	20
Computer science and techniques (cyberspace security, techniques and command)	17	20	40
Computer science and techniques (computer-equipment research, development and protection)		0	14
Internet engineering (cyberspace security, techniques and command)	35	30	45
Cyberspace security (cyberspace security, techniques and command)	0	70	60
Cryptography engineering (information research)	93	0	41
Cryptography (information management)	37	25	20
Electronic-information engineering (information-equipment techniques and protection)	0	0	11
Electronic-information engineering (information techniques and command)	0	20	11
Big-data engineering (data protection)	0	30	45
Target engineering (data protection)	0	20	45
Totals	**326**	**402**	**737**

Sources: Huangpu No. 1 Military Academy Information, '2019 Military Academy Admissions Guide 24th Station: Information Engineering University', China Military Network, 21 June 2019, http://www.chinamil.com.cn/201311jxjjh/2019-06/21/content_9535184.htm; Information Engineering University of the Strategic Support Force of the Chinese People's Liberation Army, 'Strategic Support Force Information Engineering University 2018 Recruitment Program for General High School Graduates', Qian Ye Wang website, 8 July 2018, https://www.zjut.cc/article-130162-1.html; and 'China People's Liberation Army Information Engineering University Admissions Plan 2013', BaiduWenku, 3 July 2013, https://wenku.baidu.com/view/6844bf552b160b4e767fcf31.

science, engineering, military affairs, culture and management. It has 78 distinct undergraduate programmes, though some have little to do with cyber defence. Table 2 shows a list of the majors for 2013, 2018 and 2019, and the number of students planned for recruitment in each year.[38] It appears that four new majors may have been created for 2019: artificial intelligence (AI), information security (information management), confidentiality management and electronic-information engineering. In 2019, the total number of student places for all listed cyber disciplines was 737. This

accounts for 64% of the places available at the IEU. The percentage of IEU students undertaking the cyber-related majors for 2019 is double the share for 2013, which was 34%. The number of students represents around 8% of the total number of all military-academy places available in 2019. There has been a 15% increase in overall numbers recruited for the IEU between 2013 and 2019, as well as a dramatic shift in the share of places going to the cyber disciplines. However, higher student throughput may still be too low for a country aiming to produce fully informatised armed forces by 2035. For comparison, US cyber-security education for military and national-security purposes has been the subject of concern and a succession of presidential initiatives over more than a decade. US President Donald Trump declared an arms race in cyberspace workforces in May 2019.[39] But the quality of cyber-security education in the United States is far richer than China's at every level.[40]

Based on open-source information, there is not yet a sufficient Chinese educational infrastructure to allow widespread diffusion of knowledge about cyber defence in the officer corps. Public reporting about cyber military exercises suggests a similar lack of diffusion of ideas and policies among lower-ranking personnel.

Implications of China's cyber-defence weakness

There are few probative public documents or statements from the Chinese government on different approaches to the use of force involving cyber-strike assets. Articles in military journals such as *China Military Science* (published by the PLA Academy of Military Science) or *Military Technology* (published by the National University of Defense Technology) offer some guidance, but it is impossible to determine what weight opinions published in such journals carry in leadership circles, or in formal doctrine and planning. No doubt US and allied intelligence agencies have greater insights into that question than are available in the public domain. We can, however, draw considered inferences on the basis of Chinese strategic policy.

One is that China has no intention of provoking a war, or even a short armed conflict, with the United States. This stance is unlikely to change during the next decade. China is prepared, however, to use force against

the US if needed to prevent a permanent separation of Taiwan from the mainland.[41] It would also do so to defend its current positions on disputed parts of the Spratly Islands. Of these two different scenarios, only the Taiwan crisis would be likely to involve large-scale use of cyber attacks on military targets.

Chinese leaders almost certainly believe that the United States and its allies possess overwhelming military power for most contingencies involving China, and they see superior cyber capability as underpinning that power. Partial confirmation emerges from the political, strategic and military reforms begun in 2014, which were manifested most directly in 2015 in both China's Military Strategy and its creation of the Strategic Support Force to lead and coordinate cyberspace and related information-warfare activities for the armed forces.[42] China sees itself as in the early stages of the military reforms required to be competitive in military cyberspace operations in future war, a position evidenced in part by three military goals: basic mechanisation and progress on informatisation by 2020; modernisation (including informatisation) by 2035; and top-tier global war-fighting capability by 2049.[43] Beijing also presumably envisages an AI-enabled warfare plan as part of the latter objective.[44]

Chinese planners apprehend the threats and opportunities in military uses of cyberspace in much the same way as their US counterparts. The main goal of both is information dominance. An authoritative PLA analysis, *The Science of Military Strategy*, specifically cites coordinated space, cyber and electronic warfare as strategic means to 'paralyze enemy operational system of systems and to sabotage the enemy's military command system of systems'.[45] Another source identifies targets in information warfare as including 'the enemy's information detection sources, information channels, and information-processing and decision-making systems'.[46] In a 2016 paper, Adam Segal quotes from *The Science of Military Strategy*:

> The side holding network warfare superiority can adopt network warfare to cause dysfunction in the adversary's command system, loss of control over his operational forces and activities, and incapacitation or failure of weapons and equipment – and thus seize the initiative

> within military confrontation, and create conditions for … gaining ultimate victory in war.[47]

Notwithstanding the visibility of such doctrinal views and of some organisational changes in cyber military capability, as James Johnson notes, 'far less ink has been spilled on Chinese thinking in the development of the critical support architecture, which enables and enhances China's war-fighting capabilities'.[48] In the public domain, China's military cyber-exercise scenarios and its perceptions of US target selection against China in the event of a military confrontation or related political crisis remain opaque. A recent Chinese article does suggest, however, that planners' focus has shifted from offence and early cross-domain engagement to defence and cross-domain deterrence.[49] Unsurprisingly, the author attributes the shift to 'US perceptions and practice of cyberwar'.[50]

Military academics at the PLA Air Force Engineering University have assessed that China is lagging in its development of cyber warfare compared to the United States and Russia, which have established specialised cyber-combat units with actual cyber offensive and defensive training.[51] Non-Chinese analyses are equally critical. A 2015 RAND Corporation study described China as losing out to the United States in a number of net assessments for cyber-dominated conflicts in the Taiwan Strait and in the Spratly Islands.[52] For cyber-dominated conflict, the study observed that by 2015 and looking forward to 2017, even though China had reduced the US advantage, it was still palpable.[53] Another 2015 assessment that canvassed Chinese military writings on cyberspace and asymmetric warfare concluded that 'the United States dominates cyberspace and its hegemony there is even more significant than in the real world'.[54] In a probing and significant recent contribution to understanding relative cyber military power, the authors argued that Chinese military and political leaders' dream of catching up with the US could not be achieved merely by following technological leaders, and therefore was unlikely to be realised without massive improvements in national scientific and innovation capability.[55]

Chinese political leaders probably have only a general understanding of cyber's military potential and the cyber superiority of the US alliance.

But that would be enough for them to be very cautious about approving any moves that might bring down a cyber storm on China. It is unknown whether Chinese political leaders have insisted at any stage on a position that the United States adopted in 2012, whereby only the president could authorise offensive cyber operations against other countries in peacetime. But as a result of the diplomatic tensions over cyber activities against the United States, beginning in 2013 and escalating in 2018, it is a safe assumption that Chinese leaders require a very high level of political authority in China to initiate such operations, and that they have not yet assessed, as the United States did with the Cyber Deterrence Initiative in 2018, that this authority should be passed down the chain of command. It is unlikely that China is in a position to set itself an aim for wartime, as the United States did in 2015, to devolve cyber operations to every level of command.[56] In all probability, any Chinese cyber attack against the United States would require high-level political authorisation that cannot be delegated.

Nevertheless, China's political leaders do face pressure. They know that the United States and its Five Eyes allies (Australia, Canada, New Zealand and the United Kingdom) have been conducting 'active defence' operations (non-espionage attacks) in cyberspace as part of the Cyber Deterrence Initiative to disrupt China's cyber-espionage and -reconnaissance operations, and its emplacement of militarily significant malware. The United States has also been conducting a trade war and a technology war, both launched in March 2018 and prompted in part by China's malicious activity in cyberspace. These moves threaten China's economic prosperity.[57]

As for the military leaders, the first two commanders of the Strategic Support Force have not had a solid background in cyber-warfare planning. The second of these and current commander was appointed in 2019, and had spent most of his military career in the PLA Air Force Airborne Corps. The most cyber-literate person in the command hierarchy may be one of the deputy commanders, Lieutenant-General Zheng Junjie, who has been director of the Network Systems Department since 2016, having served as president of the IEU and director of the General Staff Technical Reconnaissance Department, an intelligence-collection unit relying on cyber operations.[58]

Table 3: **Probable Chinese list of assets subject to US cyber attacks on China in a military crisis, in order of priority**

1.	Strategic nuclear-missile command and control
2.	Medium-range-missile command and control
3.	Strategic Support Force command and control
4.	Naval headquarters
5.	Eastern Theatre Command headquarters, opposite Taiwan, with primary responsibility for Taiwan contingencies
6.	Electric grids around key naval and air bases
7.	Satellite-navigation systems used by Chinese forces
8.	Naval weapons systems and platforms
9.	On-board combat systems of military aircraft
10.	Chinese intelligence, surveillance and reconnaissance capabilities

Chinese military planners surely would have compiled a list of cyber assets that are critical to national military operations in various contingencies and vulnerable to cyber attacks. The list would be a long one given the weaknesses in China's civil- and military-sector cyber defences, and its late start in planning for civil defence in cyberspace.[59] The top targets would probably include the ten listed in Table 3, many of which would also be susceptible to some form of classic electronic-warfare attacks. This list would not be highly dependent on any particular scenario.[60]

Unlike the US, China probably has not developed elaborate, computer-simulated scenarios for specific target sets. Nevertheless, China's Military Strategy 2015 indicates that the government anticipates widespread cyber disruption of its forces.[61] At the same time, Chinese military planners probably would not expect to have substantial strategic warning about where the disruptions would occur or how serious they would be for different types of units, systems and platforms.

From China's perspective, the upshot is that any armed hostilities with the United States or its allies must be as contained and brief as is politically feasible. There is clearly some tension between this imperative and China's overarching strategic priority – the use of all necessary force against Taiwan and its supporters to prevent its permanent separation from China, recognising that this may involve attacks on US military targets. To harmonise these objectives, and for other domestic political reasons, China wants to put off for as long as possible any use of force against Taiwan.[62] Thus, China sees the need for a range of coercive and subversive, but non-kinetic, measures. The crucial question it faces is whether it can apply such measures against Taiwan without provoking the US into unleashing its substantial

cyber capabilities against the Chinese armed forces and economy. While Beijing probably assesses – accurately – that the United States would seek to preserve its most advanced and secret cyber capabilities for higher-level conflict, it would be prudent for China also to judge that the US would use low- and mid-level cyber assets in a non-kinetic contingency to deter Beijing from escalating.

Segal believes that 'both the United States and China have an incentive to use cyber attacks early in a military confrontation. In addition, there are strong incentives to use the attacks broadly for denial and punishment. Every network that can support military operations is likely to be targeted.'[63] It is sensible to conclude that every such network could be targeted, but Chinese leaders would be unlikely to do so except in the most extreme circumstances. China has far less incentive than the United States to conduct the sort of military campaign in which its overall military success depends heavily on success in cyber defence.

* * *

All countries, including the United States, have appreciable weaknesses in their cyber defences. But China's are greater than those of its strategic rivals. It has a much weaker cyber-industrial base than the US, far lower levels of nationwide informatisation, a less advanced and fertile educational system, and a smaller global industrial and economic footprint. In these circumstances, new technologies such as 5G exacerbate threats. Most importantly, China has no cyber military allies, whereas the United States leads an unmatchable cyber military-alliance network.

These constraints will shape how China conducts any war with the United States and its allies. China's cyber-defence weaknesses are not likely to be manifested in asymmetric warfare across domains, involving cheap offensive cyber weapons to degrade superior US weapons platforms and systems that China cannot match. Rather, those weaknesses will probably be most salient in the balance Beijing chooses among military assets, subversion, sabotage, disruption and political pressure to push forward its strategic agenda. In particular, China appears likely to avoid reliance

on cyber strikes to disable US military assets and civilian infrastructure in favour of its better-developed assets of subversion and political warfare. In a war with the United States in the next decade, at least, China's weak cyber defences will compel it to minimise both large-scale kinetic engagements and large-scale cyber attacks on US military forces.

Acknowledgements

The author would like to acknowledge the assistance of Kai Lin Tay of the IISS in research for this article, and to thank Franz-Stefan Gady, Arthur Laudrain and Meia Nouwens for critical reviews.

Notes

1 One of the latest quantum-communication achievements from China (working with Austrian physicists) was the teleportation of multidimensional states of photons. See 'Quantum Teleportation Moves into the Third Dimension', *Physics World*, 7 August 2019, https://physicsworld.com/a/quantum-teleportation-moves-into-the-third-dimension/.

2 There are eight other Chinese Nobel laureates, but those in science (four) earned their awards either as Taiwanese (two in the 1950s) or as non-Chinese citizens (two).

3 In 2017, China had to walk away from its indigenisation plan for an operating system in favour of continued reliance on a special edition of Microsoft Windows developed for the Chinese government in a joint venture between Microsoft and a state-owned Chinese partner. See Iain Johnson, 'Redmond Puts Wall Around Windows 10 for Chinese Government Edition', 23 May 2017, *Register*, https://www.theregister.co.uk/2017/05/23/redmond_puts_wall_around_windows_10_for_chinese_government_addition/. Windows 10 is one of several US-designed software systems in common use in China providing security packages.

4 See 'President Xi Says China Faces Major Science, Technology "Bottleneck"', Xinhua, 1 June 2016, http://en.people.cn/n3/2016/0601/c90000-9066154.html.

5 See 'Bank of China Expands Relationship with IBM for Digital Transformation', IBM News Room, 27 September 2019, https://newsroom.ibm.com/2019-09-27-Bank-of-China-Expands-Relationship-with-IBM-for-Digital-Transformation.

6 IISS, 'China's Cyber Power in a New Era', *Asia-Pacific Regional Security Assessment 2019* (London: IISS, 2019), p. 90, https://www.iiss.org/publications/strategic-dossiers/asiapacific-regional-security-assessment-2019/rsa19-07-chapter-5.

7 See, for example, U.S.–China Security and Economic Review Committee, *2019 Report to Congress of the US–China Economic and Security Review Commission*, 116th Congress, 1st Session, November 2019, p. 135, https://www.uscc.gov/sites/default/files/2019-11/2019%20Annual%20Report%20to%20Congress.pdf. The report says: 'China has made great strides in key defense technologies related to cyber, space, advanced computing, and AI, and is a world leader in hypersonic weapons. Nevertheless, Beijing believes China is still lagging behind the United States, noting in its most recent defence white paper that China's military is "confronted by risks from technology surprise and a growing technological generation gap".' On p. 287, the report continues: 'Central to Beijing's new military modernization goal is the view of top civilian and military leaders that the PLA continues to lag behind the United States and other leading militaries in many elements of military power.' Also reflecting this assessment is China's own 2019 defence White Paper, which notes that although China has made 'great progress' in improving its military capabilities, the PLA has yet to complete the task of mechanisation, urgently needs to improve informatisation and 'still lags far behind the world's leading militaries'. See State Council Information Office of the People's Republic of China, 'China's National Defense in the New Era', July 2019, http://english.www.gov.cn/archive/whitepaper/201907/24/content_WS5d3941ddc6d08408f502283d.html.

8 ITU Publications, 'Global Cybersecurity Index (GCI) 2018', p. 62, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

9 Paul Bischoff, 'Which Countries Have the Worst (and Best) Cybersecurity?', Comparitech, updated 3 March 2020, https://www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country/.

10 Silja Baller, Soumitra Dutta and Bruno Lanvin (eds), *Global Information Technology Report 2016: Innovating in the Digital Economy* (Geneva: World Economic Forum, 2016), p. 16, http://www3.weforum.org/docs/GITR2016/WEF_GITR_Full_Report.pdf.

11 Cornell University, INSEAD and the World Intellectual Property Organization, 'Global Innovation Index 2019', https://www.wipo.int/publications/en/details.jsp?id=4434.

12 See China Legislation Standard, 'China Cyber Security Research Report 2018', 18 July 2019, http://www.cnstandards.net/index.php/china-cyber-security-report-2018/.

13 See Mandiant, 'APT1: Exposing One of China's Cyber Espionage Units', FireEye, 2013, https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf; and David E. Sanger, *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age* (New York: Crown, 2018). Scholar and cyber analyst Thomas Rid doubted that the Mandiant team could have pulled off such a brazen 'hackback', and publicly questioned the accuracy of Sanger's account. FireEye issued a press release stating that Sanger had mischaracterised

the operation, clarifying that it had only exploited consensual third-party security monitoring, and Sanger acknowledged that the company's clarification sounded reasonable and that he may have misunderstood key details. See Thomas Rid, 'An Imperfect Weapon', *Survival*, vol. 60, no. 5, October–November 2018, pp. 230–1; and Morgan Chalfant, 'US Cyber Firm Denies Claim It Breached Chinese Military Hackers', *Hill*, 25 June 2018, https://thehill.com/policy/cybersecurity/393994-us-cyber-firm-denies-claim-it-breached-chinese-military-hackers.

14 See Glenn Greenwald, *No Place to Hide* (New York: Metropolitan Books, 2014); and Sean Gallagher, 'Photos of an NSA "Upgrade" Factory Show Cisco Router Getting Implant', Ars Technica, 14 May 2014, https://arstechnica.com/tech-policy/2014/05/photos-of-an-nsa-upgrade-factory-show-cisco-router-getting-implant/.

15 See Office of the National Counter Intelligence Executive, 'Foreign Spies Stealing US Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage 2009–2011', Homeland Security Digital Library, October 2011, https://www.hsdl.org/?abstract&did=720057. The US government had been tracking Chinese cyber espionage since 2003, as reflected in annual reports of the National Counter Intelligence Executive, but by 2011 the United States had radically upgraded its assessment of the scale and impact of the activity.

16 'Remarks by the President in the State of the Union Address', Obama White House, 12 February 2013, https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/remarks-president-state-union-address.

17 See 'Xi Jinping Millionaire Relations Reveal Fortunes of Elite', Bloomberg News, 29 December 2012, https://www.bloomberg.com/news/articles/2012-06-29/xi-jinping-millionaire-relations-reveal-fortunes-of-elite.

18 The document trove was on a hard drive left in a journalist's post box.

19 The completed report was released in 2014, but details had been available on the ICIJ website since April 2013. See 'Secrecy for Sale: Inside the Global Offshore Money Maze', ICIJ, https://www.icij.org/investigations/offshore/.

20 For a summary, see Greg Austin, *Cyber Policy in China* (Cambridge: Polity Press, 2014), chapter four.

21 See 'Xi Jinping Leads Internet Security Group', *China Daily*, 27 February 2014, https://www.chinadaily.com.cn/china/2014-02/27/content_17311358.htm.

22 See 'Xi Jinping: Build China from a Big Network Power to a Strong Network Power', Xinhuanet, 27 February 2014, http://news.xinhuanet.com/politics/2014-02/27/c_119538788.htm.

23 State Council Information Office of the People's Republic of China, 'China's Military Strategy', China Military Online, May 2015, http://english.chinamil.com.cn/news-channels/2015-05/26/content_6507716.htm.

24 China Cybersecurity Industry Alliance, 'China's Cyber Security Industry Analysis Report 2019', December 2019, p. 2, http://www.

china-cia.org.cn/AQLMWebManage/Resources/kindeditor/attached/file//20191219/20191219092355_6832.pdf.

25 According to IBM, the 'company's key differentiators are built around three pillars – innovative technology, industry expertise, and trust and security'. IBM Security is described as the 'world's largest cybersecurity enterprise', with '8,000 subject matter experts serving more than 17,000 clients in more than 130 countries'. IBM, '2018 Annual Report', https://www.ibm.com/annualreport/assets/downloads/IBM_Annual_Report_2018.pdf.

26 'China's Cyber Security Industry Analysis Report 2019', p. 2.

27 Tencent Cyber Security Research Centre, 'Research Report on China's Industrial Internet Security Development', July 2019, p. 19, https://max.book118.com/html/2019/1011/6043232152002112.shtm.

28 *Ibid*., p. 22.

29 See Greg Austin and Wenze Lu, 'Five Years of Cyber Security Education Reform in China', in Greg Austin (ed.), *Cyber Security Education: Principles and Policies* (Abingdon: Routledge, 2020), pp. 173–93.

30 Tencent Cyber Security Research Centre, 'Research Report on China's Industrial Internet Security Development', p. 23.

31 *Ibid*., p. 19.

32 Chinese University Alumni Association, 'Alumni Association 2019 China's Top Computer Majors Ranking', 2019, http://www.cuaa.net/paihang/news/news.jsp?information_id=135786.

33 See 'Director of the Development Planning Department of the Ministry of Education: Should Explore the Dual-Mentor System for Training Cyber Security Talents', *Paper*, 17 September 2019, http://www.sohu.com/a/341380535_260616.

34 Lu Yuanzhen, 'Respond to Challenges and Build a Good Network Security Ecosystem', *Guangming Daily*, 26 August 2019, http://www.xinhuanet.com/2019-08/26/c_1124920850.htm.

35 Exploitation of 5G for cyber intrusions does not depend significantly on the country of origin of the vendor. According to the US-based Information Technology Industry Council, country of origin is only one of more than 100 potential risk factors to be considered in supply-chain security for 5G. See Information Technology Industry Council, 'ITI's 5G Policy Principles and 5G Essentials for Global Policymakers', June 2020, p. 18, https://www.itic.org/policy/ITI_5G_Full_Report.pdf.

36 According to one military source, 'the heavy use of civilian personnel has become a common practice in modern military forces and is the only way to adapt to the new military changes in the world. From the perspective of the military of developed countries in the world, the number of civilian personnel generally reaches more than half of the active duty.' 'Recruitment Announcement of the Academy of Electronic Warfare of the National University of Defence Technology in 2020', 19 October 2019, http://www.offcn.com/jzg/2019/1019/33384.html.

37 See 'The 24th Station of the 2019 Military Academy Admissions Guide: Information Engineering University', China Military Network,

21 June 2019, http://www.chinamil.com.cn/201311jxjjh/2019-06/21/content_9535184.htm.

38 See *ibid.*; Information Engineering University of the Strategic Support Force of the Chinese People's Liberation Army, 'Strategic Support Force Information Engineering University Enrollment Plan for General High School Graduates in 2018', Qianzhiwang, 8 July 2018, https://www.zjut.cc/article-130162-1.html; and 'China People's Liberation Army Information Engineering University Admissions Plan 2013', Baidu Library, 3 July 2013, https://wenku.baidu.com/view/6844bf552b160b4e767fcf31.

39 'Statement from President Donald J. Trump on America's Cybersecurity Workforce', White House, 2 May 2019, https://www.whitehouse.gov/briefings-statements/statement-president-donald-j-trump-americas-cybersecurity-workforce/.

40 See Austin (ed.), *Cyber Security Education*.

41 Trends in political relations between Taiwan and the authorities in Beijing are negative from China's point of view, especially in light of the re-election of the pro-independence President Tsai Ing-wen in January 2020. They have been deteriorating since a high point when Xi Jinping met with Ma Ying-jeou, then the nationalist president of Taiwan, in November 2015 – the first such meeting since China's civil war ended and the People's Republic of China was established in 1949. See Brendan Taylor, *Dangerous Decade: Taiwan's Security and Crisis Management*, *Adelphi* 470 (Abingdon: Routledge for the IISS, 2019).

42 See, for example, Rachel Burton and Mark Stokes, 'The People's Liberation Army Strategic Support Force: Leadership and Structure', Project 2049 Institute, 25 September 2018, https://project2049.net/wp-content/uploads/2018/09/180925_PLA_SSF_Leadership-and-Structure_Stokes_Burton.pdf.

43 See 'The Full Text of the Report of the 19th National Congress of Xi Jinping (record)', Sina Finance, 18 October 2017, http://finance.sina.com.cn/china/gncj/2017-10-18/doc-ifymvuyt4098830.shtml; and US Department of Defense, 'Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2019', 2 May 2019, p. 14, https://media.defense.gov/2019/May/02/2002127082/-1/-1/1/2019_CHINA_MILITARY_POWER_REPORT.pdf. The Pentagon notes that these goals appear regularly in PLA documents.

44 See 'With the Tide of Intelligence Coming, How Can Artificial Intelligence Subvert Future Wars?', China Science Communication, 13 August 2018, http://www.kepuchina.cn/mil/news/201808/t20180813_684798.shtml; and Yuan YiWei and Guo Yonghong, 'How to Integrate and Develop Mechanized Information and Intelligence? "Three in One" Compatibility', Chinmil.com, 12 September 2019, http://www.81.cn/jmywyl/2019-09/12/content_9619072.htm.

45 Peng Guangqian and Yao Youzhi (eds), *The Science of Military Strategy*, 3rd edition (Beijing: Military Science Press, 2013), p. 164.

46 Zhang Yuliang (ed.), *The Science of Military Campaigns* (Beijing: National Defense University Press, 2006), p. 155, cited in Larry M. Wortzel, 'The Chinese People's Liberation Army and Information Warfare', Strategic Studies Institute and US Army War College, March 2014, p. 3, https://publications.armywarcollege.edu/pubs/2263.pdf.

47 Adam Segal, 'U.S. Offensive Cyber Operations in a China–US Military Confrontation', SSRN, 15 June 2016, p. 2, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2836203.

48 James S. Johnson, 'China's Vision of the Future Network-centric Battlefield: Cyber, Space and Electromagnetic Asymmetric Challenges to the United States', *Comparative Strategy*, vol. 37, no. 5, 2018, pp. 373–90.

49 Tianjiao Jiang, 'From Offense Dominance to Deterrence: China's Evolving Strategic Thinking on Cyberwar', *Chinese Journal of International Review,* vol. 1, no. 2, August 2019, pp. 1–23.

50 *Ibid*., p. 16.

51 See Ren Meili and Du Na, 'Analysis of Network Offensive and Defensive Actions Based on Lanchester Type Equation', *National Defense Science and Technology*, no. 4, 2019, http://mall.cnki.net/magazine/article/GFCK201904021.htm.

52 Eric Heginbotham et al., *The US–China Military Scorecard: Forces, Geography, and the Evolving Balance of Power, 1996–2017* (Santa Monica, CA: RAND Corporation, 2015), https://apps.dtic.mil/dtic/tr/fulltext/u2/a621618.pdf.

53 *Ibid*., pp. 281–3.

54 Andrzej Kozłowski, 'The "Cyber Weapons Gap": The Assessment of China's Cyber Warfare Capabilities and Its Consequences for Potential Conflict over Taiwan', in D. Mierzejewski and K. Żakowski (eds), *On Their Own Paths: Japan and China Responses to the Global and Regional Challenges* (Łódź: Łódź University Press, 2015), pp. 161–72.

55 Andrea Gilli and Mauro Gilli. 'Why China Has Not Caught Up Yet: Military–Technological Superiority and the Limits of Imitation, Reverse Engineering, and Cyber Espionage', *International Security*, vol. 43, no. 3, Winter 2018/19, pp. 141–89.

56 See US Cyber Command, 'Beyond the Build: Delivering Outcomes Through Cyberspace: The Commander's Vision and Guidance for US Cyber Command', Homeland Security Digital Library, 2015, https://www.hsdl.org/?view&did=787006.

57 See Cyberspace Administration of China, 'National Cyberspace Security Strategy', translated by China Copyright and Media, December 2016, https://chinacopyrightandmedia.wordpress.com/2016/12/27/national-cyberspace-security-strategy/.

58 See Adam Ni and Bates Gill, 'The People's Liberation Army Strategic Support Force: Update 2019', *China Brief*, vol. 19, no. 10, 29 May 2019, https://jamestown.org/program/the-peoples-liberation-army-strategic-support-force-update-2019/; and Wang Jun, 'Meng Xuezheng, Head of a Certain Department of the General Staff, Succeeded Zheng Junjie as the President of PLA Information Engineering University', *Paper*, 6

May 2015, https://www.thepaper.cn/newsDetail_forward_1328391.

59 See Munish Sharma, 'India and China: Warnings Ignored?', in Greg Austin (ed.), *National Cyber Emergencies: The Return to Civil Defence* (Abingdon: Routledge, 2020), pp. 60–75.

60 See Admiral Phil Davidson, 'Transforming the Joint Force: A Warfighting Concept for Great Power Competition', speech delivered in San Diego, CA, on 3 March 2020, US Indo-Pacific Command, https://www.pacom.mil/Media/Speeches-Testimony/Article/2101115/transforming-the-joint-force-a-warfighting-concept-for-great-power-competition/. Admiral Davidson notes that the US military goal in a war with China, and therefore the foundation of the US deterrence posture, would be 'penetration and then disintegration of an adversary's systems and decision-making, thereby defeating their offensive capabilities'.

61 This is reflected in the statement: 'In response to security threats from different directions and in line with their current capabilities, the armed forces will adhere to the principles of flexibility, mobility and self-dependence so that "you fight your way and I fight my way".' State Council Information Office of the People's Republic of China, 'China's Military Strategy'.

62 See You Ji, 'Making Sense of War Games in the Taiwan Strait', *Journal of Contemporary China*, vol. 6, no. 5, June 1997, pp. 287–305.

63 Segal, 'U.S. Offensive Cyber Operations in a China–US Military Confrontation', p. 13.