# 8. China

China's leaders have moved decisively to embrace the information revolution. They started from a position of relative backwardness in electronics in the 1990s, but with the advantages of a rapidly growing economy and technology transfer from abroad. The country has since established the world's most extensive cyber-enabled domestic surveillance and censorship system, which is tightly controlled by the leadership. China's intention of becoming a cyber power was reflected in its military strategy released in 2015 and its first formal cyber-security strategy in 2016. The country has ambitious goals for the indigenous manufacture of the core internet technologies it relies on, aiming to become a world leader in such technologies by 2030. Its core cyber defences remain weak compared with those of the United States, and cyber-resilience policies for its critical national infrastructure are only in the early stages of development. China has been locked in a battle with the United States and its allies over global cyber governance since the early 2000s, a contest aggravated by US determination to sanction Chinese tech firms in response to China's malicious behaviour in cyberspace. Since the early 2000s China has conducted large-scale cyber operations abroad, aiming to acquire intellectual property, achieve political influence, carry out state-on-state espionage and position capabilities for disruptive effect in case of future conflict. China is a second-tier cyber power but, given its growing industrial base in digital technology, it is the state best placed to join the US in the first tier.

## Strategy and doctrine

China's strategic approach to the security aspects of cyberspace has been dominated by its perception of the ideological, economic and military threat from the United States: the early development of US military cyber doctrine in the 1990s; the use of cyber in US military campaigns in Kosovo in 1999 and Iraq in 2003; and US support for the internet-based political revolts in states in the former Soviet bloc and North Africa.

From the outset, China's main strategic preoccupation in cyberspace has been domestic – to prevent the spread of Western liberal thinking via the internet. From 2003 onwards, at the United Nations, it advocated the principle of 'cyber sovereignty' whereby states would be able to exert more control over their 'sovereign' portion of the internet. It was also in 2003 that China began implementing its 'Golden Shield Project', a programme of internet-based internal surveillance and censorship that became known as the Great Firewall of China – an attempt to exert sovereign control. As part of this, from 2009 onwards China undertook efforts to block certain US software applications (such as Facebook, Twitter and YouTube) because of conflicts with its censorship laws.

**List of acronyms**

| | |
|---|---|
| **BRI** | Belt and Road Initiative |
| **CAC** | Cyberspace Administration of China |
| **CCP** | Chinese Communist Party |
| **ICT** | information and communications technology |
| **MPS** | Ministry of Public Security |
| **MSS** | Ministry of State Security |
| **PLA** | People's Liberation Army |
| **SSF** | Strategic Support Force |

In 2013, after ten years of partial reforms aimed at enhancing the country's cyber capabilities, the leaders of the Chinese Communist Party (CCP) were shocked by the revelations in the leaks by US defector Edward Snowden. The leaks made clear the continuing gulf between the US and China on cyber capability, and particularly the weakness of China's cyber defences (in terms of protecting networks rather than controlling content). In 2014 President Xi Jinping instigated a wave of internet-related organisational reforms and new laws and regulations, with the aim of making China a cyber power. This included reconfiguring and assuming personal leadership of the main CCP body in charge of cyber policy[1] and establishing a new government body alongside it, the Cyberspace Administration of China (CAC). Numerous cyber-related strategies and measures for the civil sector followed. China's first national Cyberspace Security Strategy was published in 2016[2] and was supported by China's first Cybersecurity Law in 2017.[3] The strategy set nine core tasks, with a heavy emphasis on sovereignty and improving cyber-defence enablers (industry and education).[4]

On the industry side, the 'Made in China 2025' strategy, announced in 2015, is of particular significance. Identifying reliance on foreign vendors for its core internet technology as China's biggest cyber risk, this ambitious strategy intended to ensure that 70% of the core internet technology the country depended on would be manufactured domestically by 2025, and that it would become a world leader in such technology by 2030. This is complemented by the Belt and Road Initiative (BRI), in which the Digital Silk Road component is designed to open up markets in the developing world to Chinese technology.

By 2020, many of these policy measures had begun to bear fruit, including a reported decline in the incidence of domestic cyber crime.[5] But serious issues remained, including a reported doubling of intrusions into Chinese websites, with government sites a particular target.[6] Implementation of the cyber strategy has been hampered by various constraints, the biggest internal one being the low priority given to cyber-security skills in China's education system and training institutions.[7] The main external impediment has been the intensifying campaign by the US and its allies to constrain China's cyber-industrial ambitions, with the ban on sales of microchip technology to Huawei a prime example of US and allied tactics. It is not yet clear how damaging these tactics will be. They may push China to redouble its Made in China 2025 effort, to exploit the potential of its massive internal market (the country has one billion of the world's estimated four and a half billion internet users), and to step up sales of Chinese technology to the developing world through the BRI.

The other key dimension to China's cyber strategy since the early 2000s has been its use of cyber operations abroad for strategic effect. These have included industrial-scale espionage operations designed to acquire both commercial intellectual property and personal data. China has also actively used disruptive cyber operations, while being careful to pitch them below the threshold that might trigger an escalatory response – its attempts to influence electoral processes in Taiwan are one example.

China's strategy and doctrine for the military use of cyber capabilities date from the early 2000s, with its 2004 focus on 'Winning Local Wars under Informatised Conditions' an early example.[8] This strategy envisioned the incorporation of information technology into every facet of military activity, with the information domain seen not as separate but as integral to the land, air and sea domains. By 2005 this had redefined Chinese military doctrine, which stated that the protection or destruction of information systems would be a 'method of war' for the People's Liberation Army (PLA).[9]

It is important to note that Chinese military doctrine views 'network'-related activities (what most other states call 'cyber operations') as a component of information war.[10] The Chinese military sees information warfare as a struggle against adversaries to dominate the production and flow of information in order to support its strategic goals. Achieving this in a conflict environment – while degrading or constraining adversaries' efforts – is termed 'information dominance'.[11]

This is closely linked to the Chinese concept of 'systems confrontation', informed by the Chinese perception that the US defeated Iraq in the First Gulf War (1990–91) by destroying Iraq's operational command-and-control system.[12] As set out in China's *The Science of Military Strategy*, pre-emption is also a long-standing and

fundamental part of Chinese military thinking and has become even more prominent in 'information war': vulnerability to a paralysing attack on one's own command-and-control system places a premium on a first strike.[13]

This thinking has matured under Xi's leadership. One example is China's first military strategy to recognise the centrality of cyberspace in strategic and military policy, published in 2015, which stated that information would play a leading role in any conflict rather than being merely an enabler.[14] By 2019 numerous PLA sources were referring to the possibility that the acceleration of changes in military strategy, combined with new technological opportunities, would lead to an arms race in 'intelligentisation', meaning the use of artificial intelligence (AI) in military operations, intelligence collection and decision-making.[15]

**The SSF will improve China's war readiness**

The transitions foreshadowed in such doctrinal statements will take a long time to implement. As part of its aspiration to have a 'world class military' by 2050, China has set out a timetable to 2035 for the organisational reforms, including changes to force structure, that might turn doctrine into reality in the cyber realm.[16] Like the US, China is pursuing a strategy of information dominance in cyberspace, but acknowledges that its armed forces will need to undergo a transformation before that goal is reached.[17]

## Governance, command and control

Since 2014, Xi has been at the top of the chain of command for all matters concerning cyberspace, both civilian and military. His organisational changes to cyber policy in the civil and military sectors suggest that he wanted to accelerate the transformations and score some early successes in reducing the vulnerability of Chinese networks to infiltration and attack.

On the civilian side, the CAC has become the focal point of all cyberspace policy, although powerful independent nodes remain – such as the Ministry of Public Security (MPS), the Ministry of State Security (MSS) and the Ministry of Industry and Information Technology. The CAC has formalised the new agenda through national legislation and by setting up offices in each of the country's 31 provincial-level administrations.

In the military cyber sphere, in 2015 Xi established the Strategic Support Force (SSF), where most of the PLA's cyber capabilities are now centred. This was part of system-wide reforms to the PLA's force structure, administration and command-and-control mechanisms. The SSF was not a new force created from scratch but instead the result of the restructuring of existing units from across the armed forces, consolidated under a single command structure.[18] Today the SSF consists of two main elements: the Space Systems Department, responsible for space operations, and the Network Systems Department, responsible for strategic information operations.

The creation of the SSF is significant: not only does it report directly to China's paramount military decision-making body, the Central Military Commission, but it has also combined disparate capabilities into an integrated whole. Previously the PLA's information-operations units had been grouped according to mission type – namely reconnaissance, attack, defence and psychological warfare. For example, cyber espionage and signals intelligence had been handled by the now-defunct Third Department of the General Staff; offensive cyber operations and electronic countermeasures had been siloed in the former Fourth Department; psychological warfare had been the responsibility of the General Political Department; and most aspects of military network security had been managed by the General Staff Department's Informatisation Department.

Consolidating these functions into the SSF reflects the PLA's new conception of space, cyber and the electromagnetic spectrum as a unique warfighting domain rather than adjunct functions serving other forms of combat.[19] The implications of the SSF for China's military cyber capability are twofold. Firstly, a more unified force will be able to prosecute the type of complex, multidimensional information operations that the PLA foresees in future conflicts. Psychological, electronic, cyber and kinetic actions can be incorporated into a single information-warfare strategy, each deployed for specific effects at different points in a crisis or conflict.[20]

Secondly, in terms of warfighting, the SSF will improve China's war readiness and help the PLA shift more smoothly from a peacetime to a wartime

posture. By combining espionage and attack functions across electronic-, cyber- and space-warfare units, and by bringing them under a single command, the PLA aims to survey the battlefield, prepare combined-arms operations and develop specific capabilities that can be continuously adapted to match the requirements of fast-moving situations.[21] This includes malware and other cyber weapons, which can be developed, refined and deployed in a continuous loop that draws on both reconnaissance and offensive functions.

While the SSF has subsumed the PLA's strategic information-warfare units, there are still units with related functions that are attached to the single services and continue to operate within the PLA's newly created joint-theatre commands. It is unclear how effectively these units could operate alongside the SSF, and whether they have a national mission or are able to coordinate and de-conflict their respective missions during operations. According to a PLA assessment of SSF reforms, 'cross-unit forces transfer and handover are progressing smoothly; new adjustment and formation of units are being completed and delimited according to plan; the system of systems architecture and contours of new-type combat forces is starting to appear'.[22] While this authoritative assessment suggests optimism on the part of the PLA, it also indicates that reforms are at an early stage, which is likely to limit the SSF's ability to conduct multidimensional information-warfare operations in the short to medium term.

## Core cyber-intelligence capability

China has unsurprisingly organised its intelligence agencies according to its unique political system and strategic needs. The priorities of the intelligence agencies include sustaining the rule of the CCP, public order, economic and commercial intelligence, scientific and technical intelligence, military intelligence and covert operations (with the latter including political-influence operations).

These intelligence goals are pursued by competing bureaucracies. Some are stand-alone, dedicated intelligence and security agencies such as the MSS,[23] the MPS and, within the PLA, the SSF. But unlike their counterparts in Western countries, these agencies all have significant operational roles in delivering internal security. They are complemented by the intelligence-analysis work carried out by key departments of the CCP such as the Office for Taiwan Affairs, the United Front Department, the Central Cyberspace Affairs Commission,[24] the Central Commission for Politics and Law and the Central Military Commission.

Partly in reaction to the process of opening up to the world through internet access and the increase in international exchanges of all kinds, and partly because of enduring regime preferences, China has built the world's most powerful domestic surveillance system. Its domestic intelligence capability depends not just on the agencies described above but also on a complex web of enforcement mechanisms that operate in parallel. One of the most important is the Central Discipline and Inspection Commission of the CCP, which collects intelligence on leading members of the party. Another is the web of CCP committees that extends throughout all levels of government, large commercial enterprises, hospitals, schools and universities. In addition, the Golden Shield Project, launched in 2003, involves the use of information and communications technology (ICT) to transform the way China's security services collect, analyse and transmit information. China has also implemented a range of other initiatives to enhance its surveillance capabilities, including Skynet, a massive video-surveillance network that comprises at least 200 million cameras nationwide,[25] and Sharp Eyes, an extension of the Skynet network that focuses on rural areas and leverages big data and AI for social control.[26]

China also has a nationwide system that aspires to consolidate data from street-level surveillance platforms, private and public services, and the digitised records that the party-state maintains on every citizen, aiming to allow the authorities to track individuals in real time as they move across offline and online spaces. From the publicly available evidence, it is not clear how comprehensive this system is or how effective it has been.

While China's core cyber-intelligence capabilities are therefore formidable domestically, it has also developed and extensively used cyber for overseas espionage. These intelligence efforts are often characterised in terms of their volume rather than sophistication, with Chinese intrusions featuring heavily among those detected and attributed by Western intelligence agencies and cyber-security companies. That said, China

may have learned from the sophisticated Western intelligence capabilities revealed in the Snowden leaks, and may now possess more advanced capabilities either held in reserve or hidden in the sheer volume of its other operations.[27]

China's analysis and dissemination of intelligence is less mature than that of the US and its key allies. While some security officials have suggested that there is now an unmanageable glut of data generated by 'informatised' surveillance, the information ecosystem in China remains highly politicised and therefore difficult to reform. It is characterised not just by a repressive and closed institutional disposition and organisational culture, but also by the ferocity and intensity of the anti-corruption campaign that Xi has led since he took office as head of the CCP in November 2012. This campaign has purged thousands of officials from the intelligence and security agencies, including many at senior levels. Chinese intelligence analysis is very different from the systems operating in the US, the United Kingdom and in many other Western governments: it remains ideology-driven and is increasingly enmeshed with questions of prestige around the political goals of the CCP leaders, making it less independent from political influence than its Western equivalents.

## Cyber empowerment and dependence

China's participation in the globalised ICT industrial sector began in 1984 and was boosted by relationships with corporations based in the US (initially Motorola, and later Microsoft). The sector expanded dramatically once China had secured US agreement for public connectivity to the internet and the World Wide Web in 1995. A major force behind this expansion was former Chinese leader Jiang Zemin, who consistently advocated industrial transformation through electronics and information technology. By 2000, due in part to Jiang's leadership, China regarded the information society as an all-encompassing phenomenon that would be crucial for its future prosperity and security.[28] By then, the still-nascent private sector was also playing a role in the digital-technology sector, with Alibaba starting up in 1999 and the emerging computer company Lenovo getting a huge boost in 2005 when it acquired the desktop business of global tech giant IBM. Jiang's successors have subsequently increased the momentum, and under Xi there have been two particularly important developments: his 2014 declaration of China's aim of becoming a cyber power and the government launch, in 2015, of the Made in China 2025 industrial strategy.

A government white paper in 2020 stated that China had moved from a period of rapid development of its indigenous ICT industry to one in which there would be a deep and integrated digitisation of the economy and society.[29] It was not alone in this assessment. The International Monetary Fund has highlighted China's world-leading position in e-commerce and in some aspects of FinTech, describing its rate of digitisation as the fastest in the world.[30] The scale of China's value-added digital economy reached RMB 35.8 trillion (US$5.12trn) in 2019, accounting for 36.2% of GDP – a higher share than in countries such as Brazil, India and South Africa but still far behind the US (50%).[31] China's fast-expanding ICT sector was valued in 2019 at RMB 7.1trn (US$1.02trn), or just over 7% of GDP. Provinces with the most developed digital economies enjoyed the highest rates of economic growth (Beijing, Fujian, Guangdong, Shanghai and Zhejiang, for example).

China's influence in the global ICT economy has risen commensurately, including through its development of online platforms. The China Academy of Information and Communications Technology said in 2020 that with the online-platform sector, led by Alibaba and Tencent, the country's role had changed from 'imitation and catch-up' to 'leading global innovation'.[32] Before the US moved against it in 2020, the Chinese-owned company TikTok had set off a global short-video boom.

Overall, however, a large obstacle in the way of China's cyber empowerment is its ongoing dependence on foreign vendors for core internet technology, despite the Made in China 2025 strategy and indeed the emphasis science-and-technology policy has placed on self-reliance ever since the founding of the People's Republic. The Chinese media has coined the phrase 'eight guardian warriors' to refer to the US companies that remain enmeshed in China's telecommunications infrastructure: Apple, Cisco, Google, IBM, Intel, Microsoft, Oracle and Qualcomm.[33] The issue was underlined in 2020 by the US using its domination of the global microchip industry to undermine Huawei.

Indeed, in a sign that China views its reliance on foreign technology companies as likely to be long term, some of them – including Cisco, IBM, Intel and Microsoft – were invited to join China's leading consultative group for writing national standards related to cyber security. The move gives China better oversight of the use of US technology in its networks. Meanwhile, despite multiple attempts to move away from Microsoft Windows, China is yet to develop its own operating system to replace those of Microsoft or Apple.[34]

One of the technologies prioritised by Xi as part of the Made in China 2025 strategy is AI. In 2017 the government issued its first development strategy specifically for AI, aiming for China to become a world leader in the field by 2030.[35] A summary of the 14th five-year plan (2020–25), released in October 2020, emphasises investment in home-grown innovations and includes AI in a list of 'forward-looking and strategic' technologies alongside quantum communications, integrated circuits and biological engineering.[36] Chinese firms are leaders in some aspects of AI, especially concerning facial recognition, but otherwise lag far behind Microsoft and Google. The US still leads in developing the foundational platform and support architecture of AI, for example developing 66% of global AI open-source software compared with China's 13%.[37] The level of private-equity investment in AI in China is still far below that in the US, which has accounted for two-thirds of the global total since 2011.[38] China was placed second, behind the US, in a ranking of the top 50 countries according to their contributions to the two most prestigious AI conferences in 2020.[39] The story is similar for quantum computing: in 2017 Chinese scientists succeeded in entangling ten superconducting qubits, breaking Google's prior world record of nine, but since then Google has claimed a 54-qubit machine (in 2019) and IBM has developed something similar. Nevertheless, China may be a world leader in research and development (R&D) associated with quantum communications, having declared the installation of the world's longest quantum-communications cable (2,000 kilometres) between Beijing and Shanghai, as well as a connection via satellite over a smaller distance.[40] Chinese researchers announced in 2021 that a 4,600-km quantum-communications network was ready for use after two years of experimental operations.[41]

Space-based platforms related to cyber are an area where China has achieved greater self-reliance. Its total satellite fleet numbers 410.[42] It operates a large-scale space-based intelligence, surveillance and reconnaissance (ISR) capability, drawing on a fleet of 132 dedicated military satellites that is the second largest in the world after that of the US.[43] According to a 2019 report from the US Defense Intelligence Agency, China's ISR satellites are capable of offering electro-optical and synthetic aperture radar (SAR) imagery as well as electronic and signals-intelligence data.[44] They include the dual-use *Yaogan* satellite fleet[45] and the *Haiyang* series of ocean satellites, which provide global identification and tracking for military and civilian vessels.[46]

China has also developed a sovereign capability in satellite navigation through its *Beidou* system, rivalling the United States' GPS and, importantly, ending Chinese dependence on the US system for guiding its own missiles. The *Beidou* network had covered the entire Asia-Pacific region by 2012 and achieved global coverage by mid-2020. Chinese military analysts acknowledge that as China follows the US into reliance on space- and cyber-based capabilities, it will inevitably come to have the same vulnerabilities during conflict.[47]

**Chinese firms are leaders in some aspects of AI, but otherwise lag far behind Microsoft and Google**

In summary, China has made significant progress in developing an indigenous digital-industrial base but – given US dominance of global microchip supply,[48] as illustrated during the US–China trade war launched by the Trump administration – it is likely to remain fundamentally reliant on the US for its core internet technology for the foreseeable future. China has some advantages, for example an enormous internal market that provides solid foundations for winning a substantial portion of the developing world's digital market. But it is notable that in 2019, in contrast to some of his previous rhetoric, Xi described the task facing China as a new 'Long March',[49] seemingly an acceptance of the time and effort it will take to overcome the challenge posed by the US.

## Cyber security and resilience

Information security has been a priority for the Chinese government since the 1990s, yet for much of that time the focus has been on 'content security', namely the censoring of politically subversive information in cyberspace. Beijing's preoccupation with content – rather than the physical networks that transport it – reflects the party-state's conception of state security, which is more expansive and ideological than Western notions of national security. China's leaders see the security of the regime as constantly under threat.[50] It is likely that the focus on promoting content security to meet censorship objectives has diminished efforts to advance other forms of network-centred (cyber) security, and that this constraining effect will persist.

A succession of shocks has produced a sea change in China's approach to network security. In 2013, apart from the Snowden leaks, China had to deal with the humiliating exposure of a PLA cyber-espionage unit (61398) by Mandiant, a US cyber-security firm, which revealed deeply concerning gaps in the Chinese military's cyber security. Meanwhile, the eavesdropping on China's top leaders ordered by the disgraced former internal-security chief Zhou Yongkang in 2012 had highlighted the vulnerability of leadership communications and the dangers of a cyber-espionage capability beyond central control.[51]

**Beijing's own assessments of its cyber security have been sober**

Beijing's own assessments of its cyber security have been sober. A 2017 report by the National Computer Network Emergency Response Technical Team (CNCERT) stated that attacks from foreign states (advanced persistent threats) were frequent and becoming 'normal', and were directly threatening national security.[52] The report referred to serious damage to data and rampant fraud, noting that the number of attacks against industrial control systems was increasing, with many important safety incidents.[53] In September 2020, the six-monthly report released by the China Internet Network Information Center noted that personal cyber security had improved, especially in the area of online fraud, but the country's overall cyber-security situation had worsened.[54] It reported a significant increase in the number of websites affected, some of which were infected with 'backdoors'.[55] Also, the number of vulnerabilities identified in high-risk systems more than doubled from the previous year.[56]

The sheer number of new institutions, laws, regulations and announcements since 2014 suggests that China is still in the early stages of building its cyber resilience and contingency measures. Government, industry and academia have begun institutionalised exchanges through the Cybersecurity Association of China, created in 2016, which reportedly aligns the three sectors around a common set of objectives.[57] Also in 2016, Beijing announced a major reform of its national cyber-standards committee, the National Information Security Standardisation Technical Committee (NISSTC), with representatives from across government, from hundreds of Chinese companies and from a much smaller number of foreign companies. By 2018 the NISSTC had published more than 300 new cyber-security standards, covering critical-information-infrastructure protection, product review and other areas.[58] In December 2019, the Multi-level Protection Scheme 2.0 (MLPS 2.0) was implemented, broadening the scope for regulation of network operators and imposing heightened regulatory requirements.[59] To strengthen the security of its critical information infrastructure, China published 'Cybersecurity Review Measures' in 2020, outlining a set of rules to govern the review of supply-chain reliability and security underlying the products and services used by the operators of the infrastructure.[60] The government also released a draft Data Security Law in July 2020[61] and a draft Personal Information Protection Law in October 2020, representing the first comprehensive legislation relating to the security of personal data.[62]

Additionally, China's domestic cyber-security industry is much smaller than its US counterpart. Its total revenue in 2019, according to the Cybersecurity Association of China, was RMB 52.09bn (US$8.09bn),[63] which represented less than 7% of the global cyber-security industry (estimated at US$120bn in 2019).[64] The leading cyber-security firms in China have much lower revenues than those in the US, and much smaller global footprints. In the first quarter of 2020, for example, Cisco Systems, Palo Alto Networks and Fortinet respectively accounted for

9.1%, 7.8% and 5.9% of the global market[65] and the total US share was estimated at around 40%.[66]

China was ranked 27th out of 175 countries in the 2018 Global Cybersecurity Index compiled by the International Telecommunication Union (ITU).[67] Its ability to improve cyber security in the short to medium term will be constrained by its lack of a well-developed cyber-industrial complex – the enterprises, researchers and investors that help design and develop cyber-security technology. Cyber-security research and education in China is still at a basic level, with the country having no world-class universities in the field according to the Chinese University Alumni Association's 2019 ranking.[68]

## Global leadership in cyberspace affairs

Since 2002, China has engaged in efforts through the UN, the ITU and other forums to establish new international governance and norms of behaviour for cyberspace, often leading like-minded states in arguing for greater censorship and state sovereignty.[69] It has worked closely in this process with Russia and other members of the Shanghai Cooperation Organisation. Since at least 2010, when then US secretary of state Hillary Clinton made a major speech on internet freedom,[70] China has found itself locked in an ideological battle with major Western states on the human-rights and security aspects of norm-setting for cyberspace.

On rare occasions China has joined an international consensus. In 2013, for example, its representative in the UN Group of Governmental Experts (GGE)[71] supported the collective agreement that international law applied in cyberspace, and in 2015 it joined a consensus position on possible voluntary norms for cyberspace. However, China subsequently took the view that the GGE process was not adequate for its purposes and became a leader in the push for an Open-Ended Working Group (OEWG), seen as a means of diluting Western influence and allowing unfiltered participation by all states in a UN-sponsored process.[72] The OEWG was created in 2018 and began operating a year later.

China's move away from the consensus position in the UN norms forums was mirrored on the global diplomatic stage by its leadership of an agenda on global internet governance much more in line with its interests. The first step, in 2014, was its creation of the Wuzhen Internet Forum, partly in response to a series of internet-governance conferences launched in London by the UK and like-minded countries in 2011. In March 2017 the Ministry of Foreign Affairs and the State Internet Information Office published China's vision in an 'International Strategy of Cooperation in Cyberspace', stating that the 'existing global governance system of basic internet resources hardly reflects the desires and interests of the majority of countries'.[73] Central to the document was the concept of 'cyber sovereignty': while Beijing has yet to define the term explicitly, it encompasses the idea that a state should have control over networks and content within its own borders.[74] Also, in September 2020, China moved assertively to propose a 'Global Data Security Initiative' during a high-level international symposium in Beijing, in direct opposition to the United States' Clean Network programme announced a month earlier.[75] Besides advocating a 'comprehensive and objective' approach towards data-security issues, the initiative also demands respect for the 'sovereignty, jurisdiction and security management rights' of other countries, aligning with China's concept of cyber sovereignty.[76]

Domestically, Beijing has passed legislation to compel foreign companies in China to store data on domestic servers and hand over sensitive intellectual property (IP) and source code for verification and testing – examples include the State Security Law (2015) and Cybersecurity Law (2017). Other laws, for example the National Encryption Law of 2019, have further asserted China's national-security interests in terms of its control of information technologies.[77] Such regulations present obvious risks of intellectual-property theft but also exemplify the type of norms and behaviours Beijing is increasingly promoting in international forums. China is pushing for reform of international institutions such as the UN Internet Governance Forum (IGF),[78] aiming to strengthen their decision-making capacity. Beijing sees UN rule-making in cyberspace as embodying the state-led approach to cyber governance, which it favours, rather than the West's vision of relatively unrestricted information flows.[79]

The normative effect of China's cyber-governance model is becoming increasingly apparent in other

authoritarian states, such as Vietnam and Russia, which have passed strikingly similar laws on internet regulation. Beijing has enabled oppressive politics in other states through the export of surveillance technology, in which China is now an industry leader. Huawei, for example, has worked with the security forces in Zimbabwe to build voice- and facial-recognition systems, and is also widely exporting its 'smart cities' technology, whose combination of bulk data collection, storage and AI-enabled surveillance offers governments a greatly increased capacity for surveillance and social control.

Beijing has advanced its cyber interests through the Digital Silk Road, a sub-strand of the BRI. This is a geo-economic initiative aiming to place China at the centre of a global digital supply chain dominated by Chinese digital goods and services, and held together by Chinese infrastructure, technological standards, laws and regulations. Though the initiative is still in its early stages, Chinese telecoms firms already provide products and services that sit at the core of telecoms infrastructure in many countries.

Chinese IT companies enjoy significant state backing in the form of subsidies and R&D inputs, and some of them, in particular Huawei, now enjoy global leadership in 5G technology alongside Western corporations. The potential for Chinese firms to provide 5G technology to networks across the world has met with fierce resistance from some Western states, whose political elites fear the security implications of Chinese technology and its potential to be used for espionage or disruption.[80] By mid-2020 the campaign against Huawei had significantly damaged its business prospects in major developed countries but had not achieved the same impact in most other states, nor prevented the company from making a profit overall.

**Beijing has passed legislation to compel foreign companies in China to store data on domestic servers**

China now plays a powerful role in global standard-setting in emerging technologies such as the Internet of Things, Internet Protocol Version 6 (IPv6) and 5G, and Beijing has attained key positions in international standard-setting agencies such as the International Organisation for Standardisation, the International Electrotechnical Commission and the ITU.[81] However, Western and allied countries continue to exert a strong influence in this arena through their world-leading corporations. Of the 51 tech or telecoms companies in the 2020 *Fortune* 'Global 500', China had only eight; the US and its allies or close partners had the other 43.[82]

## Offensive cyber capability

China, like Russia, has made extensive use of lower-end cyber capabilities for peacetime influence-and-information operations, and thereby gained considerable experience of the relevant techniques. Based on published doctrine and proven cyber-intelligence reach, it is likely that China has also developed effective offensive cyber tools for combat use.

Though China has not published a cyber-warfare doctrine, and it may be the case that none exists,[83] authoritative PLA writings acknowledge the existence of an offensive cyber capability. The 2013 edition of *The Science of Military Strategy*, for example, dedicates a section to conflict in cyberspace and divides operations into the four categories of reconnaissance, attack, defence and deterrence, the first two of which are offensive in nature.[84] Computer reconnaissance is the use of computers to identify, monitor and analyse enemy computer networks and systems. It aims to prepare the ground in peacetime for future military operations by identifying weaknesses in adversary systems. As the requirements for successful penetration of an adversary system for reconnaissance purposes are similar to those in a 'network strike', it is possible to switch from reconnaissance to attack at the appropriate moment.[85]

The Chinese view is that network strikes could potentially follow soon after the outbreak of a conflict and would serve to disable an adversary system.[86] *The Science of Military Strategy* asserts that civilian as well as military infrastructure is a potential target during conflict, partly as the former sustains the latter but also because network strikes against civilian targets are less likely to escalate the conflict.[87] The PLA

is also considering the use of more advanced capabilities such as 'integrated network electronic warfare', which would enable it to insert malicious algorithms into an adversary network even if a wire connection does not exist. For example, Dai Qingmin, a former head of the Fourth Department of the General Staff, wrote as early as 1999 about the potential to use wireless (radio-based) cyber attacks to intercept satellites' communications or gain control over their command-and-control systems.[88]

Chinese assertions about the role and efficacy of such cyber attacks by their armed forces remain untested, so their potential impact in an actual combat engagement or war is unknown. Nevertheless, the PLA and Chinese intelligence agencies have successfully penetrated US government and commercial networks on multiple occasions, deploying malware to steal classified information and intellectual property. During a conflict the PLA's offensive cyber forces could presumably deploy similar capabilities to try to cripple the critical systems of an adversary. The knowledge acquired through past operations may also have shed light on vulnerabilities that could be exploited during wartime.[89] The PLA has both the capability and the will to penetrate adversary systems for the purpose of intelligence collection and offensive operations.

## Notes

1 This CCP body was known as the Small Leading Group on Informatisation and Cyber Security until 2018, when it was upgraded to the status of a CCP commission and renamed the Central Commission for Informatisation and Cyber Security (CCIC). This put it on a similar level to powerful entities such as the Central Military Commission. Its name in English is often shortened to the Central Cyberspace Affairs Commission (CCAC). The equivalent government body remains the Cyberspace Administration of China, which operates in part as the secretariat or office for the CCIC.

2 Cyberspace Administration of China, 'National Cyberspace Security Strategy', 2016, https://chinacopyrightandmedia.wordpress.com/2016/12/27/national-cyberspace-security-strategy.

3 Rogier Creemers, Paul Triolo and Graham Webster, 'Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)', New America, 2018, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china.

4 For an overview, see Greg Austin, *Cybersecurity in China: The Next Wave* (New York: Springer, 2018), p. 8.

5 China Internet Network Information Center, 'Statistical Report on Internet Development in China', August 2019, pp. 72–3, https://cnnic.com.cn/IDR/ReportDownloads/201911/P020191112539794960687.pdf. The report covers the first six months of 2019.

6 *Ibid*., p. 74.

7 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).

8 For an overview of the early military developments, see Greg Austin, 'China's Security in the Information Age', in Lowell Dittmer and Maochun Yu (eds), *Routledge Handbook of Chinese Security* (Abingdon: Routledge, 2015), pp. 355–70.

9 Yan Weifeng, *Cong Meijun 'konghai yiti zhan' gouxiang kan zhanyi fazhan* (Beijing: Haichao Press, 2016), p. 197.

10 Parallel concepts employed by the PLA also include 'network space' (*wangluo kongjian*) instead of 'cyberspace', and 'network warfare' (*wangluo zhan*) instead of 'cyber operations'. The PLA's dictionary of military terms defines network warfare as 'operations to destroy an enemy's network systems and network information, [and] degrade their effectiveness, while protecting one's own network systems and network information'. See Military Terminology Committee, Academy of Military Sciences, *Military Terminology of the People's Liberation Army* (Beijing: AMS Publishing, 2011), p. 286.

11 Dean Cheng, 'Winning Without Fighting: The Chinese Psychological Warfare Challenge', The Heritage Foundation, 12 July 2013, p. 2, https://www.heritage.org/global-politics/report/winning-without-fighting-the-chinese-psychological-warfare-challenge/#_ftn1.

12 Jeffrey Engstrom, 'Systems Confrontation and Systems Destruction Warfare: How the People's Liberation Army Seeks to Wage Modern Warfare', RAND Corporation, 2018, p. 10, https://www.rand.org/content/dam/rand/pubs/research_reports/RR1700/RR1708/RAND_RR1708.pdf.

13 China Aerospace Studies Institute, *In Their Own Words: Foreign Military Thought – Science of Military Strategy 2013*, 8 February 2021, pp. 58, 160–1, 221, https://www.airuniversity.af.edu/Portals/10/CASI/documents/Translations/2021-02-08%20Chinese%20Military%20Thoughts-%20In%20their%20own%20words%20Science%20of%20Military%20Strategy%202013.pdf?ver=NxAWg4BPw_NylEjxaha8Aw%3d%3d.

14 State Council Information Office of the People's Republic of China, 'China's Military Strategy', May 2015, http://eng.mod.gov.cn/Database/WhitePapers/2014.htm.

15 See, for example, 'Réngōng zhìnéng jūnbèi jìngsài zhèngzài qiǎorán xīngqǐ', *China Youth Daily*, 17 October 2019, https://m.chinanews.com/wap/detail/zw/gn/2019/10-17/8981224.shtml.

16 'Xi calls for building a strong army', Xinhua, 26 October 2017, http://www.xinhuanet.com//english/2017-10/26/c_136708142.htm.

17 See Greg Austin, 'The Strategic Implications of China's Weak Cyber Defences', *Survival: Global Politics and Strategy*, vol. 62, no. 5, September–October 2020, pp. 119–38.

18 John Costello and Joe McReynolds, 'China's Strategic Support Force: A Force for a New Era', *China Strategic Perspectives*, Institute for National Strategic Studies, National Defense University, 2018, p. 5, https://ndupress.ndu.edu/Portals/68/Documents/stratperspective/china/china-perspectives_13.pdf.

19 *The Science of Military Strategy*, produced by the PLA's Academy of Military Science, terms this development 'integrated reconnaissance, attack, and defense' [*zhen gongfang yitihua*]. See Costello and McReynolds, 'China's Strategic Support Force: A Force for a New Era', p. 12.

20 *Ibid.*, p. 40.

21 *Ibid.*, pp. 40–1.

22 'Zhànlüè zhīyuán bùduì jīcéng jiànshè gōngzuò shùpíng', Xinhuanet, 24 September 2017, http://www.xinhuanet.com/mil/2017-09/27/c_129713342.htm.

23 MSS is the main civilian intelligence and counter-intelligence agency.

24 See endnote 1.

25 Brendon Hong, 'The American Money Behind Blacklisted Chinese AI Companies', Daily Beast, 2 January 2021, https://www.thedailybeast.com/the-american-money-behind-blacklisted-chinese-artificial-intelligence-companies.

26 Josh Rudolph, 'Sharper Eyes: Surveilling the Surveillers (Part 1)', *China Digital Times*, 9 September 2019, https://chinadigitaltimes.net/2019/09/sharper-eyes-surveilling-the-surveillers-part-1.

27 Nicholas Eftimiades, *Chinese Intelligence Operations* (Abingdon: Routledge, 2017).

28 See Greg Austin, *Cyber Policy in China* (Cambridge: Polity, 2014), p. 1.

29 China Academy of Information and Communications Technology, 'Zhōngguó shùzì jīngjì fāzhǎn báipíshū', May–July 2020, pp. 49–50, http://www.caict.ac.cn/kxyj/qwfb/bps/202007/P020200703318256637020.pdf.

30 Tahsin Saadi Sedik, 'Asia's Digital Revolution', *Finance & Development*, vol. 55, no. 3, September 2018, https://www.imf.org/external/pubs/ft/fandd/2018/09/asia-digital-revolution-sedik.htm.

31 China Academy of Information and Communications Technology, 'Zhōngguó shùzì jīngjì fāzhǎn báipíshū', p. 8.

32 *Ibid.*, p. 27. Alibaba ranked 132nd in the 2020 *Fortune* Global 500 and Tencent 197th.

33 Shannon Tiezzi, 'New Report Highlights China's Cybersecurity Nightmare', *Diplomat*, 18 February 2015, https://thediplomat.com/2015/02/new-report-highlights-chinas-cybersecurity-nightmare.

34 Davey Winder, 'China Prepares to Drop Microsoft Windows, Blames US Hacking Threat', *Forbes*, 30 May 2019, https://www.forbes.com/sites/daveywinder/2019/05/30/china-prepares-to-drop-microsoft-windows-blames-u-s-hacking-threat/?sh=doa00282c50d.

35 State Council of the People's Republic of China, 'Notice of the State Council Issuing the New Generation of Artificial Intelligence Development Plan', State Council Document no. 35, 8 July 2017, https://flia.org/wp-content/uploads/2017/07/A-New-Generation-of-Artificial-Intelligence-Development-Plan-1.pdf.

36 Matt Ho, 'China's Hi-Tech Direction for the next Five Years', *South China Morning Post*, 11 November 2020, https://www.scmp.com/news/china/politics/article/3109316/chinas-hi-tech-direction-next-five-years.

37 Jeffrey Ding, 'China's Current Capabilities, Policies and Industrial Ecosystem in AI – Testimony before the U.S.–China Economic and Security Review Commission Hearing on Technology, Trade, and Military–Civil Fusion: China's Pursuit of Artificial Intelligence, New Materials, and New Energy', US–China Economic and Security Review Commission,

7 June 2019, p. 4, https://www.uscc.gov/sites/default/files/June%207%20Hearing_Panel%201_Jeffrey%20Ding_China's%20Current%20Capabilities,%20Policies,%20and%20Industrial%20Ecosystem%20in%20AI.pdf.

38 *Ibid*., p. 40.

39 Gleb Chuvpilo, 'AI Research Rankings 2020: Can the United States Stay Ahead of China?', 21 December 2020, https://chuvpilo.medium.com/ai-research-rankings-2020-can-the-united-states-stay-ahead-of-china-61cf14b1216.

40 Priyankar Bhunia, 'World's longest unhackable communications link opened between Beijing and Shanghai', OpenGovAsia, 28 October 2017, https://opengovasia.com/worlds-longest-unhackable-communications-link-opened-between-beijing-and-shanghai.

41 Liu Zhen, 'China's experiment in quantum communication brings Beijing closer to creating a hack-proof network', *South China Morning Post*, 9 January 2021, https://www.scmp.com/news/china/science/article/3117005/chinas-experiment-quantum-communication-brings-beijing-closer.

42 Union of Concerned Scientists, 'UCS Satellite Database', updated 1 January 2021, https://www.ucsusa.org/resources/satellite-database.

43 IISS, *The Military Balance 2021* (Abingdon: Routledge for the IISS, 2021), pp. 48, 191, 250.

44 Defence Intelligence Agency, 'Challenges to Security in Space', January 2019, https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Space_Threat_V14_020119_sm.pdf.

45 Andrew Tate, 'China integrates long-range surveillance capabilities', *Jane's Intelligence Review*, vol. 29, no. 12, December 2017. See also Timothy Heath, 'China's Pursuit of Overseas Security', RAND Corporation, 2018, p. 30, https://www.rand.org/content/dam/rand/pubs/research_reports/RR2200/RR2271/RAND_RR2271.pdf.

46 'Haiyang-2 (HY-2 or Ocean-2)', Globalsecurity.org, https://www.globalsecurity.org/space/world/china/hy-2.htm.

47 Kevin L. Pollpeter, Michael S. Chase and Eric Heginbotham, 'The Creation of the PLA Strategic Support Force and its Implications for Chinese Military Space Operations', RAND Corporation, 2017, p. 7, https://www.rand.org/content/dam/rand/pubs/research_reports/RR2000/RR2058/RAND_RR2058.pdf.

48 Semiconductor Industry Association, '2020 – State of the U.S. Semiconductor Industry', p. 8, https://www.semiconductors.org/wp-content/uploads/2020/07/2020-SIA-State-of-the-Industry-Report-FINAL-1.pdf.

49 'China's Xi Jinping warns of new "long march" as trade war with US intensifies', *Straits Times*, 22 May 2019, https://www.straitstimes.com/asia/east-asia/chinese-president-xi-jinping-warns-of-new-long-march-as-trade-war-intensifies.

50 Elliott Zaagman, 'Cyber Sovereignty and the PRC's Vision for Global Internet Governance', *China Brief*, vol. 18, no. 10, 5 June 2018, https://jamestown.org/program/cyber-sovereignty-and-the-prcs-vision-for-global-internet-governance.

51 Roger Faligot, *Chinese Spies: From Chairman Mao to Xi Jinping* (Melbourne: Scribe, 2019), p. 395.

52 China National Computer Network Emergency Response Team, '2016 Nián wǒguó hùliánwǎng wǎngluò ānquán tàishì zòngshù', National Computer Network Emergency Technology Processing Coordination Center, April 2017, pp. 14–20, http://www.cac.gov.cn/wxb_pdf/CNCERT2017/2016situation.pdf.

53 *Ibid*., p. 15.

54 China Internet Network Information Center, 'Statistical Report on Internet Development in China', September 2020, p. 69, https://cnnic.com.cn/IDR/ReportDownloads/202012/P020201201530023411644.pdf.

55 *Ibid*., pp. 70–2.

56 *Ibid*., p. 73.

57 Samm Sacks and Robert O'Brien, 'What to Make of the Newly Established Cybersecurity Association of China', Center for Strategic and International Studies, 25 May 2016, https://www.csis.org/analysis/what-make-newly-established-cybersecurity-association-china.

58 Samm Sacks and Manyi Kathy Li, 'How Chinese Cybersecurity Standards Impact Doing Business in China', CSIS, 2 August 2018, https://www.csis.org/analysis/how-chinese-cybersecurity-standards-impact-doing-business-china.

59 Dora Wang, Charmian Aw and Cindy Shen, 'MLPS 2.0: China's Enhanced Data Security Multi-Level Protection Scheme and Related Enforcement Updates', ReedSmith, 9 October 2019, https://www.reedsmith.com/en/perspectives/2019/10/mlps-20-chinas-enhanced-data-security-multi-level-protection.

60 Lauren Dudley et al., 'China's Cybersecurity Reviews Eye "Supply Chain Security" in "Critical" Industries [Translation]', New America, 27 April 2020, http://newamerica.org/cybersecurity-initiative/digichina/blog/chinas-cybersecurity-reviews-eye-supply-chain-security-critical-industries-translation.

61 Emma Rafaelof et al., 'Translation: China's Data Security Law (Draft)', New America, 2 July 2020, http://newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinas-data-security-law-draft.

62 Bryan Cave, 'China's Draft Personal Information Protection Law: What Businesses Should Know', Lexology, 2 December 2020, https://www.lexology.com/library/detail.aspx?g=f7f7b85c-545a-4fbe-a114-833044603750.

63 Cybersecurity Association of China (CAICT), '2020 Nián zhōngguó wǎngluò ānquán chǎnyè tǒngjì bàogà', p. 8, https://www.cybersac.cn/News/getNewsDetail/id/1545. The estimate of RMB 52.309bn is for the annual revenue from technology products and services in cyber security for companies whose revenue arising from that sector is at least 50% of their total revenue. This report includes the data from around 500 cyber-security companies in China and can be regarded as a reliable estimate compatible with similar estimates made in previous years for the sector as a whole. The CAICT has published a much higher estimate but that includes many products and services not normally included in the cyber-security sector.

64 See Gartner, 'Gartner Forecasts Worldwide Security and Risk Management Spending Growth to Slow but Remain Positive in 2020', 17 June 2020, https://www.gartner.com/en/newsroom/press-releases/2020-06-17-gartner-forecasts-worldwide-security-and-risk-managem.

65 Statista, 'Leading cybersecurity vendors by market share worldwide from 2017 to 2020', 2 July 2020, https://www.statista.com/statistics/991308/worldwide-cybersecurity-top-companies-by-market-share.

66 *Ibid*.

67 International Telecommunication Union, 'Global Cybersecurity Index 2018', p. 63, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

68 See Austin and Lu, 'Five Years of Cyber Security Education Reform in China'.

69 An overview of China's participation in debates on global norms for cyberspace can be found in Greg Austin, 'International legal norms in cyberspace: Evolution of China's national security motivations', in Anna Maria Osula and Henry Roigas (eds), *International Cyber Norms: Legal, Policy & Industry Perspectives* (Tallinn: NATO CCDCOE Publications, 2016), pp. 172–201.

70 US Department of State, 'Remarks on Internet Freedom', Hillary Rodham Clinton, Secretary of State, Washington DC, 21 January 2010, https://2009-2017.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm.

71 Since a UN General Assembly resolution in 2004, a UN Group of Governmental Experts (GGE) has convened for two-year terms to address international-security aspects of cyberspace. It was known as the GGE on 'Developments in the Field of Information and Telecommunications in the Context of International Security' until 2018, when it was renamed the GGE on 'Advancing Responsible State Behaviour in Cyberspace in the Context of International Security'. In cyberspace-policy circles it is common to refer to it simply as 'the GGE'. See UN Office for Disarmament Affairs, 'Developments in the field of information and telecommunications in the context of international security', https://www.un.org/disarmament/ict-security.

72 United Nations General Assembly, 'Resolutions adopted by the General Assembly on 5 December 2018: Developments in the field of information and telecommunications in the context of international security', Resolution 73/27, 11 December 2018, https://undocs.org/en/A/RES/73/27. The OEWG's full name is the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security. For details on its activities, see United Nations Office for Disarmament Affairs, 'Open-ended Working Group', https://www.un.org/disarmament/open-ended-working-group.

73 Tai Ming Cheung, 'The rise of China as a cybersecurity industrial power: Balancing national security, geopolitical, and development priorities', *Journal of Cyber Policy*, vol. 3, no. 3, 2018, p. 313.

74 Zaagman, 'Cyber Sovereignty and the PRC's Vision for Global Internet Governance'.

75 Chun Han Wong, 'China Launches Initiative to Set Global Data-Security Rules', *Wall Street Journal*, 8 September 2020, https://www.wsj.com/articles/china-to-launch-initiative-to-set-global-data-security-rules-11599502974.

76 China Ministry of Foreign Affairs, 'Quánqiú shùjù ānquán chàngyì', 8 September 2020, https://www.fmprc.gov.cn/web/wjbzhd/t1812949.shtml.

77 See National People's Congress of the People's Republic of China, 'Zhōnghuá rénmín gònghéguó mìmǎ fǎ (2019 nián 10 yuè 26 rì dì shísān jiè quánguó rénmín dàibiǎo dàhuì chángwù wěiyuánhuì dì shísì cì huìyì tōngguò'), 26 October 2019, http://www.npc.gov.cn/npc/c30834/201910/6f7be7dd5ae5459a8de8baf36296bc74.shtml.

78 The IGF is a multi-stakeholder discussion forum set up in 2006 in the framework of the World Summit for the Information Society, a UN body left in place after related summits in 2002 and 2003. See 'The Internet Governance Forum (IGF)', UN Internet Governance Forum, 24 June 2015, https://www.intgovforum.org/cms/2015/IGF.24.06.2015.pdf.

79 Adam Segal, 'When China Rules the Web: Technology in Service of the State', *Foreign Affairs*, vol. 7, no. 5, September–October

2018, pp. 10–14, 16–18, https://www.foreignaffairs.com/articles/china/2018-08-13/when-china-rules-web.

80 Nigel Inkster, *China's Cyber Power*, *Adelphi* 456 (Abingdon: Routledge for the IISS, 2015).

81 Kristin Shi-Kupfer and Mareike Ohlberg, 'China's Digital Rise: Challenges for Europe', MERICS Papers on China, no. 7, April 2019, p. 21, https://merics.org/sites/default/files/2020-06/MPOC_No.7_ChinasDigitalRise_web_final_2.pdf.

82 For the tech companies in the 2020 *Fortune* Global 500 ranking, see 'Global 500', *Fortune*, https://fortune.com/global500/2020/search/?sector=Technology. For the telecoms companies, see 'Global 500', *Fortune*, https://fortune.com/global500/2020/search/?sector=Telecommunications.

83 Kevin Pollpeter, 'Chinese Writings on Cyberwarfare and Coercion', 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).

84 Amy Chang, 'Warring State: China's Cybersecurity Strategy', Center for a New American Security, December 2014, p. 25, https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/CNAS_WarringState_Chang_report_010615.pdf?mtime=20160906082142&focal=none.

85 Joe McReynolds, 'China's Evolving Perspectives on Network Warfare: Lessons from the Science of Military Strategy', *China Brief*, vol. 15, no. 8, April 2015, p. 5, https://jamestown.org/program/chinas-evolving-perspectives-on-network-warfare-lessons-from-the-science-of-military-strategy.

86 Pollpeter, 'Chinese Writings on Cyberwarfare and Coercion', p. 7.

87 McReynolds, 'China's Evolving Perspectives on Network Warfare: Lessons from the Science of Military Strategy', p. 5.

88 Pollpeter, 'Chinese Writings on Cyberwarfare and Coercion', p. 8.

89 *Ibid.*, pp. 13–14.