On the Asymmetric Advantages of Cyberwarfare. Western Literature and the Chinese Journal Guofang Keji

Journal:	*Journal of Strategic Studies*
Manuscript ID	FJSS-2018-0156.R2
Manuscript Type:	Original Article
Keywords:	Cyberwarfare, China, Asymmetric Warfare, Assassin's Mace, Guofang Keji

SCHOLARONE™
Manuscripts

On the Asymmetric Advantages of Cyberwarfare.
Western Literature and the Chinese Journal *Guofang Keji*

Abstract. An issue that has been widely debated in the West is whether cyberwarfare gives militarily weaker actors asymmetric advantages. Is cyberwarfare a weapon of the weak? Or does it rather multiply the advantages enjoyed by militarily superior actors? These questions have major implications for China, which – as a rising power – must face stronger and weaker opponents at the same time. Based on an analysis of the Chinese journal *Guofang Keji*, this article investigates how China's strategic community theorises advantage and disadvantage in the cyber domain and how this differs from Western perspectives on cyberwarfare.

Keywords. Cyberwarfare – China – Asymmetric Warfare – Assassin's Mace – *Guofang Keji*.

For Peer Review Only

Over the past two decades, cyberspace has rapidly emerged as a new arena of international competition.[1] Yet, whether and how the military exploitation of the new domain is transforming international politics remains a highly contentious issue. One particular question that has received considerable attention among scholars and analysts is whether the new technology favours militarily weaker actors or stronger ones. On the one hand, many (especially in policy circles) view cyberwarfare as a weapon of the weak: a strategic equaliser that empowers smaller nations and non-state actors in their fight against stronger enemies. On the other hand, others (especially in academia) are sceptical about the equalising potential of the new technology, which some even conceive as just the opposite: a weapon of the strong that amplifies the advantage enjoyed by militarily superior actors *vis-à-vis* their weaker opponents.

This theoretical debate has major implications for China. As a rising power, China is confronting both stronger and weaker opponents at the same time. On the one hand, it must cope with challenges originating from above in the hierarchy of power, where the United States is increasingly alarmed by the emergence of a potential competitor.[2] On the other hand, it continues to face resistance from below, where smaller powers embroiled in territorial and maritime disputes with Beijing have an interest in derailing its rise.[3] If the new technology works as a weapon of the weak, cyberwarfare

[1] For an early assessment of the new domain's impact on international politics and International Relations theory, see Andreas Wenger (ed.), "The Internet and the Changing Face of International Relations and Security", special issue, *Information & Security* 7 (2001). Over the past two decades, the implications of the cyber phenomenon for International Relations theory have been widely debated: to limit references to books, see for instance David J. Betz and Tim Stevens, *Cyberspace and the State. Toward a Strategy for Cyber-Power* (London: IISS 2011), 35-74; Nazli Choucri, *Cyberpolitics in International Relations* (Cambridge, MA: MIT Press 2012), 25-48; Chris C. Demchak, *Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security* (Athens, GA: University of Georgia Press 2011), 22-47; Johan Eriksson and Giampiero Giacomello (eds.), *International Relations and Security in the Digital Age* (London: Routledge 2007); Jan-Frederik Kremer and Benedikt Müller (eds.), *Cyberspace and International Relations. Theory, Prospects and Challenges* (Belin: Springer 2014); Nye, Joseph S., *The Future of Power* (New York: Public Affairs 2011), 113-51.

[2] On China as a rising power and its implications for Sino-U.S. relations, see for instance the debate on the so-called 'Thucydides trap': Graham Allison, 'The Thucydides Trap: Are the U.S. and China Headed for War?', *The Atlantic* (September 24, 2015), https://www.theatlantic.com/international/archive/2015/09/united-states-china-war-thucydides-trap/406756/; Graham Allison, *Destined for War. Can America and China Escape Thucydides's Trap?* (Boston, MA: Houghton Mifflin Harcourt 2017); James R. Holmes, 'Beware the "Thucydides Trap" Trap. Why the U.S. and China Aren't Necessarily Athens and Sparta or Britain and Germany before WWI', *The Diplomat* (June 13, 2013), https://thediplomat.com/2013/06/beware-the-thucydides-trap-trap/; Gregory J. Moore, 'Avoiding a Thucydides Trap in Sino-American Relations (… and 7 Reasons Why that Might be Difficult)', *Asian Security* 13/2 (2017), 98-115.

[3] On China's rise and the implications for Beijing's relations with its neighbours, see the debate on balancing vs. bandwagoning in East Asia: Evelyn Goh, 'Great Powers and Hierarchical Order in Southeast Asia: Analyzing Regional

For Peer Review Only

will increase China's leverage against stronger rivals, including the U.S., all while intensifying China's own vulnerability to attacks from weaker enemies. By contrast, if the new technology works as a weapon of the strong, cyber threats to China's national security will mostly originate from other great powers and the U.S. in particular, while Beijing's own advantage *vis-à-vis* its weaker enemies will be further consolidated.

Recent developments in the military doctrine and force structure of the People's Liberation Army (PLA) suggest that the cyber domain is expected to play a major role in the future of China's national defence. In 2015, China's white paper on military strategy for the first time identified cyberspace as a 'critical security domain' (*zhongda anquan lingyu*), along with the oceans, outer space and the nuclear domain.[4] At the end of the same year, the PLA Strategic Support Force (PLASSF) was established as a specialized force for developing and operating China's space and cyber capabilities. A wide range of space, cyber and electronic warfare assets previously under separate PLA institutions were then transferred to the PLASSF, which is now in charge of both information support and information warfare.[5] With the PLA increasingly focused on the cyber domain, it is crucial to understand the similarities and differences between Western and Chinese perspectives on cyberwarfare.

The aim of this article is to ascertain whether the way in which cyberwarfare is theorised within China's strategic community is consistent with either of the two opposing views underlying debate in the West. Do China's analysts theorise cyberwarfare as a weapon of the weak? Do they emphasise the new opportunities that cyberspace creates for China *vis-à-vis* the U.S.? Or do they

---

Security Strategies', *International Security* 32/3 (2008), 113-57; David C. Kang, *China Rising. Peace, Power, and Order in East Asia* (New York, NY: Columbia U.P. 2007), 50-75; Robert S. Ross, 'Balance of Power Politics and the Rise of China: Accommodation and Balancing in East Asia', *Security Studies* 15/3 (2006), 355-95. For more recent contributions to this debate, see G. John Ikenberry, 'Between the Eagle and the Dragon: America, China, and Middle State Strategies in East Asia', *Political Science Quarterly* 131/1 (2016), 9-43; Adam P. Liff, 'Whither the Balancers? The Case for a Methodological Reset', *Security Studies* 25/3 (2016), 420-59; Robert S. Ross and Øystein Tunsjø (eds.), *Strategic Adjustment and the Rise of China. Power and Politics in East Asia* (Ithaca, NY: Cornell U.P. 2017).

[4] Zhonghua Renmin Gongheguo Guowuyuan Xinwen Bangongshi (Information Office of the PRC State Council), *Zhongguo de Junshi Zhanlüe* (China's Military Strategy) (Beijing: Renmin Chubanshe 2015), 11-2.

[5] On the PLASSF see 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* (Santa Monica, CA: RAND Corporation 2017); Rachael Burton and Mark Stokes, *The People's Liberation Army Strategic Support Force. Leadership and Structure* (Arlington, VA: Project 2049 Institute 2018); John Costello and Joe McReynolds, *China's Strategic Support Force: A Force for a New Era* (Washington, D.C.: National Defense University Press 2018); Elsa B. Kania and John K. Costello, 'The Strategic Support Force and the Future of Chinese Information Operations', *The Cyber Defense Review* 3/2 (2018), 105-21.

URL: http://mc.manuscriptcentral.com/fjss
For Peer Review Only

rather perceive cyberwarfare as a weapon of the strong, with a focus on U.S. cyber threats to China's national security? To answer these questions, this article analyses how cyberwarfare is discussed in the Chinese journal *Guofang Keji* (Science and Technology for National Defence). Established in 1978, *Guofang Keji* is published by the National University of Defence Technology (*Guofang Keji Daxue*, NUDT), the PLA academic institution in charge of 'cultivating advanced scientific, technological and command talents, training high-level cadres of the military and engaging in research on advanced weaponry and key technologies for national defence'.[6] Authored not only by scholars based at NUDT but also by military analysts based at other PLA institutions, the articles in *Guofang Keji* offer important insights into the perceptions and preferences of China's strategic community.[7]

This article is organised as follows. The first section describes the two Western perspectives outlined above. As we shall see, they rest on opposing assumptions about three crucial issues raised by the advent of cyberwarfare: whether the cyber domain's barriers to entry are low or high; whether strong actors are more or less vulnerable to cyberattacks than their weaker opponents; and whether cyber weapons should be used independently or combined with traditional military force. In the second and third sections, these three dimensions of the Western debate are used to explore the *Guofang Keji* discourse, as we analyse how the Chinese authors address each of the three issues and whether this corresponds to either of the two perspectives underlying the Western debate. The conclusions provide an assessment of how cyberwarfare is theorised in *Guofang Keji*, how this differs from the debate occurring in the West, and the implications for China's approach to the new domain.

1. The Western debate

Let us start with a discussion of the two perspectives introduced above: the argument that cyberwarfare favours weak actors, which we will call the 'weapon of the weak discourse', and the argument that cyberwarfare favours strong actors instead, or the 'weapon of the strong discourse'.

[6] Zhongguo Da Baike Quanshu – Junshi Bianweihui (Editorial Committee of 'Chinese Encyclopedia – Military'), *Zhongguo Da Baike Quanshu – Junshi* (*Chinese Encyclopedia – Military*) (Beijing: Zhongguo Da Baike Quanshu Chubanshe 2005), 923. In 2017 NUDT was reorganised to absorb several pre-existing academic institutions: the Chinese name was also changed from *Guofang Kexue Jishu Daxue* to *Guofang Keji Daxue*. See Ying Yu Lin, 'One Step Forward, One Step Back for PLA Military Education', *China Brief* 18/7 (2018), https://jamestown.org/program/one-step-forward-one-step-back-for-pla-military-education/.

[7] For a preliminary analysis of a sample of *Guofang Keji* articles in the context of a study on U.S.-China relations in cyberspace, see Author 2018.

URL: http://mc.manuscriptcentral.com/fjss
For Peer Review Only

This is not to imply that everything that has been written in the West on cyberwarfare can be reduced to either of these two discourses. Yet the issue of whether the new technology favours the weak or the strong has been a recurrent topic in Western literature and as such it has significantly oriented the debate. For this reason, a focus on this dichotomy will help to identify a fundamental dimension of how Western scholars have conceptualized and discussed cyberwarfare. According to Jon R. Lindsay, the idea that cyberwarfare is a 'weapon of the weak' is one of the basic assumptions behind the 'Cyber Revolution' thesis, i.e. the belief that the new technology will radically alter the way international politics works. Although widely influential in the policy community, this thesis is less popular in academia, as scholars 'have generally (but not exclusively) been skeptical of the notion that the internet revolutionizes war'.[8] Sketched in this section as ideal types, the weapon of the weak and the weapon of the strong discourses will be used in the rest of the article to compare the way in which cyberwarfare is debated in the West with the way it is theorised in *Guofang Keji*.

The weapon of the weak discourse is based on a set of interrelated assumptions regarding the three issues mentioned above: the cyber domain's barriers to entry, weak and strong actors' relative vulnerability to cyberattacks, and the feasibility of independent cyberwarfare. First, the cyber domain's barriers to entry are presented as very low. Cyber weapons are cheaper than other military technologies because an effective cyberattack can be launched even with rudimentary equipment. Barriers to entry are further lowered by the dual-use nature of cyber technology, which makes it easier for weak actors to develop military capabilities in cyberspace.[9] Second, strong actors are assumed to be more vulnerable than weak ones. Technologically advanced militaries are relatively more dependent on networks and this creates vulnerabilities that weak actors will exploit to compensate for their overall inferiority.[10] Such a dependence–vulnerability nexus is true not just for the military

[8] Jon R. Lindsay, 'Stuxnet and the Limits of Cyber Warfare', *Security Studies* 22/3 (2013), 365-404, 368.

[9] Stephen Blank, 'Web War I: Is Europe's First Information War a New Kind of War?', *Comparative Strategy* 27/3 (2008), 227-47; Lucas Kello, 'The Meaning of the Cyber Revolution. Perils to Theory and Statecraft', *International Security* 38/2 (2013), 7-40; Gregory D. Koblentz and Brian M. Mazanec, 'Viral Warfare: The Security Implications of Cyber and Biological Weapons', *Comparative Strategy* 32/5 (2013), 418-34; Kenneth Lieberthal and Peter W. Singer, *Cybersecurity and U.S.-China Relations* (Washington, DC: Brookings, 2012); Gary McGraw, 'Cyber War is Inevitable (Unless We Build Security In)', *Journal of Strategic Studies* 36/1 (2013), 109-19; Joseph S. Nye, 'Nuclear Lessons for Cyber Security?', *Strategic Studies Quarterly* 5/4 (2011), 18-38; Nye, *The Future of Power*, 122-32; Dale Peterson, 'Offensive Cyber Weapons: Construction, Development, and Employment', *Journal of Strategic Studies* 36/1 (2013), 120-24; Derek S. Reveron, 'An Introduction to National Security and Cyberspace', in Derek S. Reveron (ed.), *Cyberspace and National Security. Threats, Opportunities, and Power in a Virtual World* (Washington, DC: Georgetown U.P., 2012), 3-19.

[10] John Arquilla, 'Cyberwar Is Already Upon Us. But Can It Be Controlled?', *Foreign Policy*, February 2012, 27, http://foreignpolicy.com/2012/02/27/cyberwar-is-already-upon-us/#; David C. Gompert and Martin Libicki, 'Waging

For Peer Review Only

but for society at large, as vital civilian infrastructures are run by industrial control systems that are exposed to cyberattacks. On such infrastructure, defence is extremely complicated for several reasons, including the existence of multiple points of entry, difficult coordination among the several actors involved in cyber defence, and the problem of correctly attributing cyberattacks.[11] Third, it is assumed that cyber weapons can be used independently to achieve strategic effect. Cyberattacks against vital civilian targets will impose high costs on the enemy: the 'potency of cyber weapons' is such that this could even happen without resulting in physical destruction. Cyber is then conceived as an autonomous military domain where war should be waged independently from operations in the 'terrestrial' domains of land, sea and air.[12] At a military disadvantage in traditional domains, weak actors will capitalise on their advantage in cyberspace to overturn the overall balance of forces. The new technology thus favours those powers that oppose the strong actor *par excellence*: the United States. This is the case with 'rogue states' such as Iran and North Korea and with rival great powers such as Russia.[13] But states are not the main beneficiaries of cyber weapons: barriers to entry are so low that the new technology will empower the weakest among the weak – non-state actors, including terrorist groups, criminal networks and even individuals.[14] In fact, the diffusion of cyber technology is expected to trigger a structural transformation of international politics: 'the cyber revolution's

For Peer Review Only

Cyber War the American Way', *Survival* 57/4 (2015), 7-28; McGraw, 'Cyber War is Inevitable'; Greg Rattray, *Strategic Warfare in Cyberspace* (Cambridge MA: MIT Press 2001), 34-64.

[11] On the vulnerability of vital civilian infrastructures see McGraw, 'Cyber War is Inevitable'; Peterson, 'Offensive Cyber Weapons'. On the offense-dominant nature of cyberspace, see for instance Arquilla, 'Cyberwar Is Already Upon Us'; Kello, 'The Meaning of the Cyber Revolution'; Nye, 'Nuclear Lessons'. On the attribution problem, see Richard B. Andres, 'The Emerging Structure of Strategic Cyber Offense, Cyber Defense, and Cyber Deterrence', in Reveron (ed.), *Cyberspace and National Security*, 89-104; Kello, 'The Meaning of the Cyber Revolution'; Koblentz and Mazanec, 'Viral Warfare'; Lieberthal and Singer, *Cybersecurity and U.S.-China Relations*.

[12] Kello, 'The Meaning of the Cyber Revolution'; for a more articulated discussion of strategic cyberwarfare and its preconditions, see Rattray, *Strategic Warfare*, 101-51.

[13] Nikolas K. Gvosdev, 'The Bear Goes Digital. Russia and Its Cyber Capabilities', in Reveron (ed.), *Cyberspace*, 173-89; Richard R. Kugler, 'Deterrence of Cyber Attacks', in Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz (eds.), *Cyberpower and National Security* (Washington, DC: National Defense U.P. 2009), 309-40; Timothy L. Thomas, 'Nation-State Cyber Strategies: Examples from China and Russia', in Kramer, Starr and Wentz (eds.), *Cyberpower*, 465-88. On the cyber (or 'informational') component of Russia's 'cross-domain coercion strategy', see Dmitry (Dima) Adamsky, 'From Moscow With Coercion: Russian Deterrence Theory and Strategic Culture', *Journal of Strategic Studies* 41/1-2 (2018), 33-60. On a North Korean attempt at cyber coercion, see Travis Sharp, 'Theorizing Cyber Coercion: The 2014 North Korean Operation Against Sony', *Journal of Strategic Studies* 40/7 (2017), 898-926; for an alternative assessment of the same operation, see Christopher Whyte, 'Ending Cyber Coercion: Computer Network Attack, Exploitation and the Case of North Korea', *Comparative Strategy* 35/2 (2016), 93-102.

greatest dislocations, in the end, may be felt not in the balance of power but in the balance of players'.[15]

These conclusions are rejected in the weapon of the strong discourse, which is based on a different set of assumptions. First, it is assumed that the cyber domain's barriers to entry are not low. Although elementary cyberattacks may be launched with rudimentary equipment, achieving significant political goals requires considerable resources. A case in point is *Stuxnet*, whose success was in fact based on the mobilisation of huge financial and organisational resources over a protracted period of time.[16] Second, although strong actors do depend heavily on networks, taking advantage of such vulnerability is not easy. A major obstacle is the complexity that permeates cyberspace as much as any other operational domain: deviation from normal organisational standards, messy working practices and human mistakes provide the defender with additional (albeit accidental) protection from attack, which means that cyberwarfare is less offence-dominant than is usually assumed. When it comes to cyber defence, strong actors might be better positioned than their weaker opponents owing to the greater resources that they possess, including in addressing the issue of attribution.[17] Third, cyber weapons are most effective not when employed independently but when used in support of traditional military force. What the attacker might achieve by targeting enemy networks is nothing more than a temporary advantage: to transform this into a long-term shift in the balance of forces, the attacker needs to complement cyberwarfare with more traditional, 'terrestrial' forms of military action. Cyberattacks are therefore most effective when they form part of an 'offline-online interaction'. If

---

[14] Andres, 'The Emerging Structure'; Blank, 'Web War I'; Steven Bucci, 'Joining Cybercrime and Cyberterrorism. A Likely Scenario', in Reveron (ed.), *Cyberspace and National Security*, 57-68; Nye, 'Nuclear Lessons'; Reveron, 'An Introduction'; Kello, 'The Meaning of the Cyber Revolution'.

[15] Kello, 'The Meaning of the Cyber Revolution', 190. See also Nye, *The Future of Power*, 132-51.

[16] Adam P. Liff, 'Cyberwar: A New "Absolute Weapon"? The Proliferation of Cyberwarfare Capabilities and Interstate War', *Journal of Strategic Studies* 35/3 (2012), 401-28; Jon R. Lindsay, 'Stuxnet'; Thomas Rid, *Cyber War Will Not Take Place* (London: Hurst & Company 2013), 44-5, 115, 169-70. See also David Betz, 'Cyberpower in Strategic Affairs: Neither Unthinkable nor Blessed', *Journal of Strategic Studies* 35/5 (2012), 689-711; Max Smeets, 'A Matter of Time: On the Transitory Nature of Cyberweapons', *Journal of Strategic Studies* 41/1-2 (2018), 6-32. On *Stuxnet* see also James P. Farwell and Rafal Rohozinski, 'Stuxnet and the Future of Cyber War', *Survival* 53/1 (2011), 23-40; Rebecca Slayton, 'What Is the Cyber Offense-Defense Balance?: Conceptions, Causes, and Assessment', *International Security* 41/3 (2016/17), 72-109.

[17] On offence-dominance as a myth see Lindsay, 'Stuxnet'; Rid, *Cyber War Will Not Take Place*, 167-9. In fact, according to Rebecca Slayton, the offence–defence balance in cyberspace is not systemic but dyadic, i.e. 'a characteristic not of cyberspace, but rather of the relationship between two adversaries': Slayton, 'What Is the Cyber Offense-Defense Balance?', 107. On attribution see Thomas Rid and Ben Buchanan, 'Attributing Cyber Attacks', *Journal of Strategic Studies* 38/1-2 (2015), 4-37.

URL: http://mc.manuscriptcentral.com/fjss
For Peer Review Only

this is the case, cyberwarfare is an option only when traditional military capabilities are also in place: it follows that 'cyberwar should be particularly appealing to capable states confronting weaker opponents'.[18] This was the case with *Stuxnet*, and the same conclusion can be drawn from the 2007 and 2008 cyber campaigns against Estonia and Georgia attributed to Russia.[19] The systemic implications of cyber technology are then just the opposite of those postulated in the weapon of the weak discourse: far from triggering a process of power diffusion, cyber weapons consolidate the existing hierarchy of power by widening the gap between strong and weak actors.

The polarisation between these two discourses tends to be reflected in the way Western analysts look at China's role in cyberspace. Advocates of the weapon of the weak discourse are convinced that, in the new domain, China holds asymmetric advantages over the United States. Owing to its greater dependence on information flows and the vulnerability of its networks, the U.S. is particularly exposed to cyberattacks.[20] By contrast, China has developed advanced defence capabilities, with strict governmental control over the Internet resulting in a supposed 'capacity to isolate the mainland's entire network from the global web'.[21] In addition, China has superior offensive capabilities because it is better at mobilising 'non-state cyber capabilities' in the form of cyber militias.[22] On the other hand, research on China's cyber doctrine offers a more nuanced picture of how Beijing perceives the military balance in the cyber domain. While still emphasising China's view of cyber weapons as asymmetric assets, these studies have made clear that Beijing considers

[18] Erik Gartzke, 'The Myth of Cyberwar. Bringing War in Cyberspace back down to Earth', *International Security* 38/2 (2013), 41-73, 63. On 'offline-online interaction' see Johan Eriksson and Giampiero Giacomello, 'Conclusion. Digital-Age Security in Theory and Practice', in Erkisson and Giacomello (eds.), *International Relations and Security in the Digital Age*, 173-84, 180. See also Betz and Stevens, *Cyberspace and the State*, 88-97; Betz, 'Cyberpower in Strategic Affairs'. On 'operational cyberwar' as a more viable option than 'strategic cyberwar' see Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica: RAND 2009), 117-58; on the fact that 'Information Warfare Only Looks Strategic' see also Martin C. Libicki, *Conquest in Cyberspace. National Security and Information Warfare* (Cambridge: Cambridge U.P. 2007), 37-49. On the fact that cyberwarfare is not an efficient option for terrorists see Giampiero Giacomello, 'Bangs for the Buck: A Cost-Benefit Analysis of Cyberterrorism', *Studies in Conflict & Terrorism* 27/5 (2004), 387-408.

[19] Gartzke, 'The Myth of Cyberwar'.

[20] See Joel Brenner in Joel Brenner and Jon R. Lindsay, 'Debating the Chinese Cyber Threat', *International Security* 40/1 (2015), 191-95; George P. Manson III, 'Cyberwar: The United States and China Prepare for the Next Generation of Conflict', *Comparative Strategy* 30/2 (2011), 121-33; Adam Segal, 'Chinese Computer Games: Keeping Safe in Cyberspace', *Foreign Affairs* 91/2 (2012), 14-20; Timothy L. Thomas, 'Google Confronts China's "Three Warfares"', *Parameters* 40/2 (2010), 101-13. On U.S. vulnerability to China's 'information warfare stratagems' see Thomas, 'Nation-State Cyber Strategies'.

[21] Manson, 'Cyberwar', 124.

[22] Alexander Klimburg, 'Mobilizing Cyber Power', *Survival* 53/1 (2011), 41-60.

URL: http://mc.manuscriptcentral.com/fjss
For Peer Review Only

itself to be in a position of overall inferiority *vis-à-vis* the United States in the new domain.[23] What these studies suggest is that widespread concerns about China's impact on U.S. cybersecurity may be grossly exaggerated: according to Lindsay, 'the magnitude of the gap between China and the United States in the balance of cyber power […] is potentially growing, not shrinking'.[24]

2. The *Guofang Keji* discourse

We will now turn to *Guofang Keji* and the way in which cyberwarfare is theorised in the Chinese journal. In order to assess whether this theorisation fits with the weapon of the weak or the weapon of the strong discourse, we start by focusing our analysis on how Chinese authors discuss the cyber domain's barriers to entry, the relative vulnerability of weak and strong actors, and the feasibility of independent cyberwarfare.

To start with, Chinese authors are convinced that barriers to entry are low. As argued in a 2013 article, 'the threshold of the technology used in cyberwar is low, [therefore,] the establishment of cyberwar forces and the acquisition of fighting strength are fast'.[25] First, if compared with conventional or nuclear technology, cyber technology has 'low costs and high returns' (*di chengben, gao huibao*). Second, the technology used in a cyberattack does not differ substantially from the technology used for civilian purposes, so that 'cyberwar can quickly enlist troops and develop capabilities through societal recruitment, school training and similar channels'.[26] For these reasons,

[23] For a recent discussion of China's cyber doctrine based on the extensive analysis of Chinese sources, see Dean Cheng, *Cyber Dragon. Inside China's Information Warfare and Cyber Operations* (Santa Barbara: Praeger 2017). According to Cheng, China's approach to cyberwarfare is more correctly qualified as 'orthogonal', i.e. an approach that implies a completely different set of assumptions and goals: see Cheng, *Cyber Dragon*, 207-08. For other analyses based on Chinese sources, see also Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron (eds.), *China and Cybersecurity. Espionage, Strategy, and Politics in the Digital Domain* (Oxford: Oxford U.P. 2015) and especially the following contributions: Kevin Pollpeter, 'Chinese Writings on Cyberwarfare and Coercion', 138-62; Robert Sheldon and Joe McReynolds, 'Civil-Military Integration and Cybersecurity. A Study of Chinese Information Warfare Militias', 188-222; Mark A. Stokes, 'The Chinese People's Liberation Army Computer Network Operations Infrastructure', 163-87; and Ye Zheng, 'From Cyberwarfare to Cybersecurity in the Asia-Pacific and Beyond', 123-37.

[24] Jon R. Lindsay, 'The Impact of China on Cybersecurity. Fiction and Friction', *International Security* 39/3 (2015), 7-47, 44. See also Cheng, *Cyber Dragon*, 215.

[25] Guo Fuliang, Yang Xinde and Zhou Gang, 'Wai Jun Wangluo Zhan Fazhan Xiankuang Yanjiu ji Qishi' ('Analysis and Assessment of the Current Situation of Cyberwar Development in Foreign Armed Forces'), *Guofang Keji* 34/3 (2013), 49-52, 51.

[26] *Ibid*.

URL: http://mc.manuscriptcentral.com/fjss
For Peer Review Only

offensive capabilities in the new domain can easily be developed by a wide range of actors, including not only 'less developed countries' but also terrorist groups, companies and even individuals.[27] Unlike many of their Western colleagues, however, Chinese authors do not consider low barriers to entry equivalent to a level playing field. As one author explains, 'because of the gap between levels of economic, scientific and technological development, the gap between the military cyber capabilities of different countries is an objective reality'.[28] While low barriers to entry allow both strong and weak actors to develop military capabilities in the cyber domain, their effectiveness in doing so is still decisively influenced by the overall gap in terms of economic and technological resources.

Against this background, the actor that stands to benefit most from the new technology is in fact the United States. Cyberspace is mostly analysed not just in its military dimension but as a comprehensive domain whose economic, political, cultural and military dimensions are inextricably intertwined. In this broadly defined domain, the U.S. enjoys overwhelming superiority that *Guofang Keji* presents as 'absolute' (*juedui*) or, alternatively, as 'general' (*zongti*), 'comprehensive' (*zhengti*) or 'strategic' (*zhanlüe*).[29] It is the advantage that comes with the superior economic resources controlled by the U.S. and its greater technological prowess: as the 'birthplace of the Internet',[30] the United States exerts 'monopolistic' (*longduan*) dominance over much of the information technology

[27] *Ibid*.; Sun Wei and Bao Chuang, 'Guoji Wangluo Anquan Chanpin Shichang Fazhan Xianzhuang yu Qushi' ('State of Development and Trends of the International Market for Cybersecurity Products'), *Guofang Keji* 37/2 (2016), 59-64; Zhang Jianchao, Shen Xueshi and Zhong Hua, 'Mei Jun Wangluo Kongjian Zuozhan Lilun Fazhan ji Yingxiang Fenxi' ('Analysis of the Impact and Development of the U.S. Military Cyberspace Operations Theory'), *Guofang Keji* 37/3 (2016), 63-7; Zheng Hebin, 'Wangluo Junbei dui Zhuquan de Yingxiang ji Woguo Duice' ('The Impact of Cyber Arms on Sovereignty and Countermeasures of China), *Guofang Keji* 34/2 (2013), 62-8; Wang Zengzhuo and Zhu Yajie, 'Mei Jun Wangluo Silingbu yu Guojia Anquan Ju Chaifen de Kenengxing' ('On the Possibility of a Split between the U.S. Cyber Command and the National Security Agency'), *Guofang Keji* 39/5 (2018), 91-6.

[28] *Ibid*., 64.

[29] Du Yanyun and Liu Yangyue, 'Zhong Mei Wangluo Kongjian Boyi yu Jingzheng' ('Sino-U.S. Game and Competition in Cyberspace') *Guofang Keji* 35/3 (2014), 70-82; Guo, Yang and Zhou, 'Wai Jun Wangluo Zhan Fazhan'; Ke Hongfa, Zhu Jilu and Zhao Rong, 'Tuijin Wangluo Kongjian Hexin Zhiyuan Nengli Jianshe' ('Promoting the Building-Up of Core Supporting Capabilities in Cyberspace'), *Guofang Keji* 38/2 (2017), 50-4; Liang Meng, Han Yue and Qiao Zheng, 'Meiguo "Guofangbu Wangluo Kongjian Zuozhan Zhanlüe" Shuping' ('A Discussion of the U.S. "Department of Defence Strategy for Operating in Cyberspace" '), *Guofang Keji* 33/1 (2012), 84-7; Sun Wei, 'Quanli Zhengzhi Shijiao Xia Wangluo Zhuquan de Jichu' ('The Basis of Cyber Sovereignty from the Perspective of Power Politics'), *Guofang Keji* 37/6 (2016), 81-7; Sun and Bao, 'Guoji Wangluo Anquan Chanpin'; Zhuang Lin and Si Huijing. 'Meiguo Wangluo Anquan Zhanlüe de Shizhi' ('Essence of the U.S. Cybersecurity Strategy'), *Guofang Keji* 34/4 (2013), 74-8.

[30] Chen Tian, Xian Ming and Li Zili, 'Mei Jun Wangluo Kongjian Zuozhan Guihua Yanjiu' ('Research on the Planning of U.S. Cyber Warfare'), *Guofang Keji* 37/3 (2016), 68-72, 68.

URL: http://mc.manuscriptcentral.com/fjss
For Peer Review Only

that other countries depend on to develop their own cyber capabilities.[31] Such superiority is at the root of Washington's 'Internet hegemony' (*wangluo baquan*).[32] This is reflected in U.S. superiority when it comes to the military uses of the cyber domain, where Washington benefits from interactions between the military and a dynamic private sector.[33] The U.S. thus holds an indisputable advantage over any other actor: it enjoys unrestricted 'Internet dominance' (*zhi wang quan*) and 'occupies the high ground' (*qiangzhan zhigaodian*) in the military competition in cyberspace.[34] In this context, China is structurally at a disadvantage and remains 'on the whole in a weak position'.[35] Over the past 15 years, Beijing has made considerable progress in technological development, achieving major breakthroughs in areas where it enjoys an 'advantage of the follower' (*hou fa youshi*), including global positioning systems and supercomputers.[36] But this is not enough and the country still lags behind the U.S., especially when it comes to the application of the new technologies to the military sphere, with substantial delays in doctrinal development and force construction.[37] Inferiority *vis-à-vis* the U.S. thus persists, posing a major challenge to China's national security. The Prism programme is often mentioned as proof that Washington is already capitalising on its superiority in the new domain to extract information from China.[38]

For Peer Review Only

[31] Fu Yanhong and Zhao Yang, 'Wangluo Kongjian Junbei Kongzhi Yanjiu Xianzhuang ji Qishi Sikao ('State of Research on Cyberspace Arms Control and Assessment'), *Guofang Keji* 34/1 (2013), 34-7; Wu Zecheng, 'Meiguo Wangluo Baquan dui Zhongguo Guojia Anquan de Yingxiang ji Duice' ('The Influence of U.S. Cyber Hegemony on China's National Security and Countermeasures against It'), *Guofang Keji* 35/1 (2014), 55-60; Zhan Xiaosu, 'Jiaqiang Wangluo Guofang Jianshe Zhanlüe Yunchou Xuyao Qianghua de Liu Zhong Yishi' ('On the Six Elements of Awareness that Should Be Strengthened in order to Reinforce the Strategic Planning for Cyber National Defence Construction'), *Guofang Keji* 34/6 (2013), 69-72.

[32] Du and Liu, 'Zhong Mei Wangluo'; Fu and Zhao, 'Wangluo Kongjian Junbei Kongzhi'; Guo, Yang and Zhou, 'Wai Jun Wangluo Zhan'; Liang, Han and Qiao, 'Meiguo'; Wu, 'Meiguo Wangluo Baquan'; Zheng, 'Wangluo Junbei'.

[33] Huo Jiajia, 'Meiguo Wangluo Fangwu Chengbao de Xianzhuang' ('State of Cyber Defence Contracting in the United States'), *Guofang Keji* 37/6 (2016), 100-03; Cai Jun and Yu Xiaohong, 'Meiguo Wangluo Kongjian Zuozhan Nengli Jianshe' ('On the Construction of U.S. Cyberspace Operations Capabilities), *Guofang Keji* 39/3 (2018), 105-9. On cooperation between the U.S. military, civilian agencies and private companies see also Liu Yangyue, 'Jun Min Ronghe Shijiao Xia de Meiguo Wangluo Anquan Rencai Zhanlüe' ('U.S. Strategy for Cybersecurity Personnel From the Point of View of Civil-Military Fusion'), *Guofang Keji* 39/1 (2018), 71-5.

[34] Wu, 'Meiguo Wangluo Baquan', 58-59. See also Du and Liu, 'Zhong Mei Wangluo'.

[35] *Ibid.*, 72. See also Zhan, 'Jiaqiang Wangluo Guofang Jianshe'.

[36] Du and Liu, 'Zhong Mei Wangluo'.

[37] Wu, 'Meiguo Wangluo Baquan'.

Looking at *Guofang Keji*, China's threat perception in the cyber domain seems to be dominated by a focus on the U.S. and its 'life-and-death power'.[39] Little room is left for weaker actors, with a marginal role attributed to those actors that dominate much of the Western debate: non-state actors. The articles in *Guofang Keji* do recognise that 'using information attack and defence technology and using the Internet to organise and conduct terrorist activities has become everyday practice for all kinds of terrorist organisations'.[40] And yet, non-state actors are not presented as major players in the cyber arena but are relegated to a separate dimension: the sphere of so-called 'non-traditional security' (*fei chuantong anquan*), where terrorists are associated with religious extremists and national separatists.[41] If non-state actors play a marginal role, small powers are completely out of the picture: for instance, *Guofang Keji* articles never identify China's neighbours as posing a cyber threat to national security. The only two East Asian countries that are sporadically mentioned are Japan and South Korea, but both of them as technologically advanced powers whose cyber capabilities are well ahead of China's.[42]

If we move to the relative vulnerability of weak and strong actors, Chinese authors are convinced that strong actors are more vulnerable than weaker ones. This has to do, first of all, with their greater dependence on information and communication technology. The Revolution in Military Affairs has increased the importance of information flows in technologically advanced militaries so that their combat effectiveness would be significantly degraded if the enemy were able to interfere with military information networks. According to one *Guofang Keji* article, this can be done in four different ways: by disrupting the enemy's 'command information systems', thus interfering with the decision-making process; by infiltrating its 'military information network' for intelligence purposes; by intruding into the 'weapon control network' in order to degrade the enemy's combat readiness; and by exploiting 'backdoor loopholes' in order to paralyse its air defence system.[43] The U.S. military

[38] Chen, Xian and Li, 'Mei Jun Wangluo'; Du and Liu, 'Zhong Mei Wangluo'; Huo, 'Meiguo Wangluo Fangwu'; Wu Tong, 'Jingwai Xinxi Wangluo Jiankong Xingshi yu Tiaozhan' ('Situation and Challenges of Information Network Monitoring Abroad'), *Guofang Keji* 37/3 (2016), 40-3; Wu, 'Meiguo Wangluo Baquan'; Zhan, 'Jiaqiang Wangluo Guofang Jianshe'; Zhuang and Si, 'Meiguo Wangluo Anquan'.

[39] Du and Liu, 'Zhong Mei Wangluo', 71.

[40] Hu Yanjing and Zhan Zhongkun, 'Jiakuai Tuijin Xinxi Gongfang Xinxing Zuozhan Liliang Jianshe' ('On Speeding Up the Construction of the New Combat Force of Information Attack and Defence'), *Guofang Keji* 38/2 (2017), 64-7, 66.

[41] Zhang, Shen and Zhong, 'Mei Jun Wangluo'.

[42] Du and Liu, 'Zhong Mei Wangluo'; Guo, Yang and Zhou, 'Wai Jun Wangluo Zhan'; Sun, 'Quanli Zhengzhi Shijiao Xia'; Sun and Bao, 'Guoji Wangluo Anquan Chanpin'; Wu, 'Meiguo Wangluo Baquan'; Zheng, 'Wangluo Junbei'.

[43] Tian Chengxin, Zhang Feng and Jiang Fei, 'Wangluo Zhan dui Zuozhan de Yingxiang ji Duice' ('Influence of Cyberwarfare on Operations and Countermeasures'), *Guofang Keji* 35/5 (2014), 103-05, 104.

URL: http://mc.manuscriptcentral.com/fjss
For Peer Review Only

is particularly exposed to similar 'hidden dangers' (*yinhuan*), so that a major cyberattack against its networks would have severe repercussions.[44] In developed countries, however, it is not just the military that depends heavily on networks. Like their Western colleagues, Chinese authors insist on wider societal dependence as an element of intrinsic vulnerability. According to a 2009 article, technologically advanced societies rely on a set of 'crucial infrastructures' (*guanjianxing jichu sheshi*), including the electric grid, communication and transportation networks, and financial services: if these 'strategic weak points' (*zhanlüe ruodian*) are hit, society as a whole will be paralysed.[45] A 'new mode of military operations' is then theorised: 'information and infrastructure warfare' (*xinxi he jichu sheshi zuozhan*), a form of cyberwarfare that specifically targets vital civilian infrastructure. A campaign of this kind was reportedly launched by Russia during the 2008 war against Georgia, although it had only a limited impact due to Georgia's low level of 'internetisation' (*wangluohua*). But things would be different if similar operations were conducted against more advanced societies: in particular, the U.S. would be extremely vulnerable to this form of warfare.[46]

While pointing to U.S. vulnerabilities, some *Guofang Keji* articles also express concern for China's own increasing dependence on networks. Due to China's rapid economic development, its 'information infrastructures and information systems have increased in terms of numbers, expanded in terms of scope, and become more complicated in terms of architecture'. Defending such infrastructures and systems is becoming more and more difficult, with major implications for China's national security. In this respect, 'crucial services' that have undergone full 'informatisation' and 'internetisation', including in the financial, transportation and energy sectors, are particularly problematic.[47] While this is common to all advanced economies, what makes China more vulnerable than the developed countries is its heavy reliance on foreign technology. As mentioned in a 2017 article, China is still dependent on imports for 'information technology core products' (*xinxi jishu hexin chanpin*) such as chips and operating systems.[48] Similarly, a 2014 article warned that China's four major banks use CISCO equipment in their data centres and that the same U.S. company provides much of the equipment used in Chinese customs, public security and education bureaus, and in the

[44] Zhuang and Si, 'Meiguo Wangluo Anquan'.

[45] Cheng Shaojie, Zhang Tao and Chang Zhenyu, 'Wangluo Kongjian yu 21 Shiji de "Shouzhan" ' ('Cyberspace and "First Strike" in the Twenty-First Century'), *Guofang Keji* 30/6 (2009), 81-4, 82.

[46] Shang Liang, Yang Guoxin, Shi Jinlai and Sui Shilong, 'Wangluo Zhan Budui. Ge Guo Jun Zhong Xin Chong' ('Cyberwar Forces: The New Favourite of Every Country's Military'), *Guofang Keji* 30/4 (2009), 89-92.

[47] Wu Chenggang, 'Jiakuai Zhongguo "Wangluo Guofang" Jianshe de Zhanlüe Sikao' ('Strategic Reflection on Accelerating the Construction of China's "Cyber National Defence" '), *Guofang Keji* 33/3 (2012), 1-4.

[48] Hu and Zhan, 'Jiakuai Tuijin Xinxi Gongfang', 64.

URL: http://mc.manuscriptcentral.com/fjss
For Peer Review Only

railways, civil aviation and oil sectors.[49] As noted in the 2017 article, 'while private use is not a big problem, the fact that vital national institutions such as the government and the military extensively use foreign products might pose a serious threat to our information security, national defence security and state security'. In particular, the use of foreign technology makes it more difficult for China to protect its cyber infrastructure because 'installing security products and protection measures on platforms developed by others is like building a tower on shifting sand'.[50]

The greater vulnerability of stronger actors is exacerbated by the offence-dominant nature of cyberwarfare. Chinese authors agree that offence has an advantage over defence, and that defending against a cyberattack remains a prohibitive task even for stronger actors, despite their superior technological and financial resources. The only effective way to protect sovereignty in cyberspace is through cyber offence, with the cyber forces conceived as quintessentially 'offensive combat units' (*gongjixing zuozhan danwei*).[51] This is confirmed to Chinese authors by the fact that even the U.S. – the cyber 'hegemon' – has opted for an offensive approach. As noted in a 2016 article, '"threat" is the most common word in any sort of U.S. strategic document on cyberspace and, accordingly, strengthening the defence of cyberspace security is presented as the primary mission: still, in relying on its technological monopolistic advantage, the U.S. military remains convinced that "the best defence is attack"'.[52]

If we finally move to the feasibility of independent cyberwarfare, the articles in *Guofang Keji* theorise both an independent and an integrated use of cyber weapons. As argued in a 2017 article, 'depending on a mission's requirements, [our cyber forces] should be able to fight freely and flexibly, or to fight perfectly integrated and coordinated with any other armed service or corps, thus strengthening their information warfare capabilities and increasing the accuracy of [their] armaments'.[53] However, while discussing the employment of cyber forces to support traditional

[49] Du and Liu, 'Zhong Mei Wangluo'.

[50] Hu and Zhan, 'Jiakuai Tuijin Xinxi Gongfang', 64.

[51] Tang Lu, 'Qianxi Yi Falü Xingshi Kongzhi Wangluo Junbei Jingsai de Biyaoxing' ('An Analysis on the Necessity of Controlling Cyber Arms Race through Law'), *Guofang Keji* 31/3 (2010), 33-6, 35. See also Ke, Zhu and Zhao, 'Tuijin Wangluo Kongjian'. On the impact of new technological developments on the offence-defence balance in cyberspace, see Shen Xueshi, 'Wangluo Kongjian Gong Fang Jishu Fazhan Dongxiang Fenxi' ('An Analysis of the Development Trends in Cyberspace Offence and Defence Technology'), *Guofang Keji* 38/4 (2017), 42-6.

[52] Zhang, Shen and Zhong, 'Mei Jun Wangluo Kongjian', 66. See also Du and Liu, 'Zhong Mei Wangluo'; Ma Zengjun and Li Jian, 'Mei Jun Wangluo Zuozhan Zhihui yu Kongzhi de Guoqu, Xianzai yu Jianglai' ('Past, Present and Future of the U.S. Cyberwarfare Command and Control'), *Guofang Keji* 35/5 (2014), 73-85; Sun and Bao, 'Guoji Wangluo Anquan Chanpin'. Nevertheless, a 2018 article notes that defence is recognised a greater role in recent U.S. documents: Wang and Zhu, 'Mei Jun Wangluo Silingbu'.

[53] Hu and Zhan, 'Jiakuai Tuijin Xinxi Gongfang', 66.

URL: http://mc.manuscriptcentral.com/fjss
For Peer Review Only

operations, this and other articles also contemplate independent cyberwarfare as a way to have a strategic effect. On the one hand, cyberattacks can be used to paralyse the enemy's armed forces, resulting in their collapse even if no significant victory has been achieved in any other domain. On the other hand, wider effects can be obtained if cyberattacks are directed against civilian targets, thus breaking the morale of the population and forcing the enemy to surrender before large-scale fighting has even started. As noted in the same 2017 article, 'by attacking the electric grid, water reservoirs, communication and energy infrastructures, the result of "not fighting – or fighting only a small war – and subduing the enemy" [*bu zhan huo xiao zhan er qu ren zhi bing*] can be achieved'.[54] Interestingly, cyberattacks against civilian targets are thus framed as a modern application of Sun Zi's celebrated principle of 'not fighting and subduing the enemy' (*bu zhan er qu ren zhi bing*) – an indirect way of achieving strategic effect without resorting to open military force.[55] This is the reason why Chinese authors expect that future wars will inevitably start with cyberattacks as a 'first shot' (*shou zhan*). According to a 2009 article, 'winning war in the future will probably depend on successfully launching and winning a "cyber first shot" [*wangluo shou zhan*]'.[56] The cyber domain will thus come to play a decisive role in war: as argued in other articles, 'whoever controls this battlefield will seize the initiative in the wars of the future',[57] as 'superiority in cyberspace will decide superiority in all other dimensions'.[58]

3. Assassin's mace vs. strategic equaliser

If we go back to the two discourses laid out in the first section, the analysis of *Guofang Keji* paints an apparently contradictory picture. The Chinese discourse on cyberwarfare seems to present

[54] *Ibid*., 65.

[55] Sun Zi's principle of 'not fighting and subduing the enemy' is mentioned in other *Guofang Keji* articles. See also: Tang, 'Qianxi Yi Falü Xingshi'; Xiao Xunlong and Li Shouqi, 'Wangluo Yulun Zhan de Lilun Tanxi' ('Theoretical Analysis of Cyber Public Opinion Warfare'), *Guofang Keji* 35/2 (2014), 5-8; Yang Tengfei, Zhu Yaohua and Zhang Weichao, 'Heping Shiqi Wangluo Yulun Zhan de Tedian ji Duice Chuyi' ('Observations on the Characteristics of and Countermeasures to Cyber Public Opinion Warfare in Peacetime'), *Guofang Keji* 35/2 (2014), 33-6; Cai and Yu, 'Meiguo Wangluo Kongjian'. For a critical discussion of the principle of 'not fighting and subduing the enemy' in Chinese ancient military thought, see Alastair Iain Johnston, *Cultural Realism. Strategic Culture and Grand Strategy in Chinese History* (Princeton, N.J.: Princeton U.P. 1995), 99-105.

[56] Cheng, Zhang and Chang, 'Wangluo Kongjian', 84.

[57] Zhang, Shen and Zhong, 'Mei Jun Wangluo Kongjian', 66.

[58] Wu, 'Jiakuai Zhongguo', 2.

URL: http://mc.manuscriptcentral.com/fjss
For Peer Review Only

ingredients of both the weapon of the weak and the weapon of the strong discourse. On the one hand, Chinese authors are convinced that the new domain has low barriers to entry and that this favours weak actors. They assume that strong actors are generally more vulnerable to cyberattacks, as their militaries and societies depend more heavily on the flow of information. In addition, they theorise an independent use of the new technology, with strategic cyberwarfare compensating for the overall military inferiority of weak actors. On the other hand, however, Chinese authors emphasise the advantage that the United States – the strong actor *par excellence* – enjoys in the cyber domain. In their view, although barriers to entry are low, only strong actors have the financial and technological resources to capitalise on the cyber phenomenon. In this respect, China remains at a disadvantage *vis-à-vis* the U.S., and the gap between the two is actually widening rather than closing. According to *Guofang Keji*, such a disadvantage is further exacerbated by China's reliance on foreign technology, which makes it more difficult for Beijing to protect its national cyber infrastructure. What is particularly disorienting in this discourse – if we look at it through the lens of debate in the West – is the way how the United States is perceived. In *Guofang Keji*, the superpower is systematically presented as both a threat and a target. On the one hand, the U.S. emerges as the major cyber threat to China's national security: faced with a China that is on the rise in economic, diplomatic and military terms, Washington is reportedly leveraging the new domain to preserve its hegemonic position. On the other hand, in much of *Guofang Keji*'s discussion of China's cyber campaigns, the U.S. is also the implicit target: with stronger actors relatively more vulnerable to cyberattacks and with independent cyberwarfare as a strategic option, China has every incentive to exploit the new domain in order to close the power gap with the U.S.

There is a logic behind this apparent contradiction. *Guofang Keji* authors always assume a distinction between two different types of superiority in the cyber domain: general superiority and 'local superiority' (*jubu youshi*). The former is the comprehensive advantage that one side enjoys in terms of the overall power distribution in cyberspace, including not just the military dimension but also the political, economic and cultural ones. Local superiority, by contrast, is a more specific form of superiority that is limited in both space and time. It is the advantage enjoyed by one side within the context of a specific conflict, with its peculiar characteristics in terms of political motivation, psychological conditions, economic resources, military capabilities etc. This distinction between general and local superiority is a consolidated principle of China's doctrinal thinking. The relative nature of superiority and inferiority is in fact a key component of China's solution to a long-standing strategic problem, namely how to 'defeat the superior from a position of inferiority' (*yi lie sheng you*),

For Peer Review Only

a concern that has been central to the military doctrine of the PLA since its formative years and continues to remain so under the current 'conditions of informatisation'.[59]

Needless to say, the side holding the general advantage does not necessarily hold the local advantage in a specific conflict. When the *Guofang Keji* authors argue that the U.S. enjoys 'absolute superiority', they refer to superiority in the broader distribution of power within the new domain. Still unchallenged in its technological primacy, the U.S. exerts a cyber hegemony that poses a comprehensive and multi-dimensional threat to China's national security. However, the fact that China remains at a disadvantage in the 'overall situation' (*quanju*) does not mean that the new domain is inevitably unfavourable to Beijing: superiority can still be established 'locally' (*jubu*). In case of a conflict, China should first 'destroy the opponent's information superiority or prevent such a superiority from producing its results'.[60] Then it should 'seize the strategic high ground in the cyber confrontation and thus progressively gain superiority in the *local* competition around cyber national defence'.[61] Once such local superiority has been gained, China will turn to 'asymmetric' (*feiduichen*) cyberattacks against the enemy. According to *Guofang Keji*, these attacks should be directed at both military and civilian targets. If U.S. military networks are 'paralysed' through asymmetric cyberattacks, the entire U.S. military effort will be significantly affected.[62] In this respect, a particularly promising arena for cyberattacks is air defence: 'under conditions of informatisation', a 'powerful cyberattack from the technologically inferior side' could inflict severe damage on the air defence systems of a technologically more advanced enemy, thus opening the way for large-scale air campaigns.[63] At the same time, the weaker side should target the enemy's critical civilian

[59] Deng Feng, 'Bianzheng Renshi Gao Jishu Zhanzheng Zhong Yi Lie Sheng You de Wenti' ('Dialectical Understanding of the Issue of Defeating the Superior from a Position of Inferiority in High-Tech Wars'), *Zhongguo Junshi Kexue* 17/3 (2004), 107-11; Jiang Lei, *Xiandai Yi Lie Sheng You Zhanlüe* (Contemporary Strategy for Defeating the Superior from a Position of Inferiority) (Beijing: Guofang Daxue Chubanshe 1997); Ning Jun and Dan Xiufa, 'Mao Zedong Yi Ruo Sheng Qiang Lilun Zai Yanjiu' ('New Research on Mao Zedong's Theory of the Defeating the Strong from a Position of Weakness'), *Zhongguo Junshi Kexue* 23/3 (2010), 60-70; Sun Qiangyin, 'Zhunque Tangxun Xinxihua Zhanzheng Yi Lie Sheng You Zhisheng Jili' ('Exploring the Mechanism of Defeating the Superior from a Position of Inferiority in Informationized War'), *Guofang Keji* 36/1 (2015), 75-8. For an authoritative statement of the relative nature of 'superiority' and 'inferiority', see Junshi Kexueyuan Zhanlüe Yanjiubu (Academy of Military Sciences Strategy Research Institute), *Zhanlüe Xue* (*The Science of Military Strategy*) (Beijing: Junshi Kexue Chubanshe 2001), 459.

[60] Hu and Zhan, 'Jiakuai Tuijin Xinxi Gongfang', 66.

[61] Zhan, 'Jiaqiang Wangluo Guofang Jianshe', 71, emphasis added.

[62] Wu, 'Jiakuai Zhongguo'.

[63] Huang Renquan and Li Weimin, 'Kongfang Duikang Zhanchang Tuozhan Dao Wang Dian Kongjian dui Weilai Guojia Fangkong de Yingxiang' ('The Extension of the Air Defence Battlefield to Cyberspace: Impact on the Future of National Antiaircraft Defence'), *Guofang Keji* 33/3 (2012), 46-50, 48.

URL: http://mc.manuscriptcentral.com/fjss
For Peer Review Only

infrastructure in order to break the morale of the civilian population and secure a rapid victory. Thus, the 'information and infrastructure warfare' mentioned above is theorised as a quintessentially strategic form of warfare with a 'decisive impact in accomplishing the war goals'.[64]

By virtue of their strategic potential, cyber weapons are then theorised in *Guofang Keji* as 'assassin's maces' (*shashoujian*) – the term used in Chinese doctrinal writings to identify a wide range of high-tech weapons that enable a weaker actor to confront a stronger enemy.[65] Although the weaker side remains in a condition of overall inferiority, the deployment of an assassin's mace increases its combat effectiveness considerably in the local confrontation. As argued in the 2001 edition of *Science of Military Strategy*, the authoritative doctrinal publication of the PLA Academy of Military Sciences, a well-designed 'high + low combination' of advanced and backward weapon systems will have a multiplying effect with a '1 + 1 > 2' result.[66] Western analysts have long recognised that cyber weapons are identified in China as an asymmetric assassin's mace:[67] what is worth emphasising here, however, are the implications of such an identification for our comparison between the *Guofang Keji* discourse and the Western debate on cyberwarfare. At first glance, the assassin's mace might appear to be a Chinese synonym for the 'strategic equaliser' theorised in the weapon of the weak discourse. Both the assassin's mace and the strategic equaliser assume the feasibility of independent cyberwarfare and the potential that the new technology has to close the power gap between a weak and a strong actor. Yet the two concepts differ greatly in terms of barriers to entry, with the assassin's mace being much more demanding in this respect than the strategic equaliser. In the weapon of the weak discourse, cyber weapons are conceived as a strategic equaliser in the sense that such weapons can be easily developed by any actor, including small nations and non-state groups. By contrast, the assassin's mace discussed in *Guofang Keji* is not equally accessible to all.

In the Chinese discourse, there are two requirements for a weak actor to develop an assassin's mace. First, it has to make a major breakthrough in a key area of technological innovation. As argued

[64] Cheng, Zhang and Chang, 'Wangluo Kongjian', 83.

[65] For a detailed discussion of the concept of *shashoujian* see Jason Bruzdzinski, 'Demystifying *Shashoujian*: China's "Assassin's Mace" Concept', in Andrew Scobell and Larry Wortzel (eds.), *Civil-Military Change in China: Elites, Institutes, and Ideas After the 16th Party Congress* (Carlisle, PA: Strategic Studies Institute 2004), 309-64. See also Dennis J. Blasko, '"Technology Determines Tactics": The Relationship Between Technology and Doctrine in Chinese Military Thinking', *Journal of Strategic Studies* 34/3 (2011), 355-81; Jacqueline Newmyer, 'The Revolution in Military Affairs with Chinese Characteristics', *Journal of Strategic Studies* 33/4 (2010), 483-504.

[66] Junshi Kexueyuan Zhanlüe Yanjiubu, *Zhanlüe Xue*, 459.

[67] For instance see Manson, 'Cyberwar'; Nigel Inkster, *China's Cyber Power* (London: Adelphi Series 2015), 95-6; Lindsay, 'The Impact of China'; Pollpeter, 'Chinese Writings'.

URL: http://mc.manuscriptcentral.com/fjss
For Peer Review Only

in *Guofang Keji*, if China wants to take advantage of the cyber domain, it must first 'break technological shortcomings and overcome weak points' by gaining mastery of the 'key technologies' used in command, control, computers and communication systems.[68] Second, at the same time, the weak actor must raise the overall level of its technological sophistication. As emphasised by Chinese authors, an assassin's mace is not just a matter of 'deciding victory or defeat based on a couple of new weapons'.[69] With the transformation of warfare from a struggle between platforms into a struggle between complex systems, a new weapon will remain unable to play the role of a true assassin's mace unless it is fully integrated into the overall 'informationised weapon system'.[70]For this reason, developing an assassin's mace requires not just progress in a specific technology but also the generalised upgrading of the entire system.

From this point of view, the assassin's mace works as a weapon of the weak in a much more qualified way than the strategic equaliser because it remains out of reach for most weak actors and especially for non-state ones. In turn, this has major implications when it comes to the structural potential of the two concepts. While the strategic equaliser theorised in the weapon of the weak discourse is expected to drive a power diffusion process that could drastically reshape international order, the impact of the assassin's mace is much more limited. Far from triggering an apocalyptic collapse of the state-centric international order, cyber weapons as conceived in *Guofang Keji* will rather shift the military balance at the top of the international hierarchy by facilitating a rising power's challenge to the hegemon.

Conclusions

The analysis presented above suggests that the way in which cyberwarfare is theorised in *Guofang Keji* does not match any of the two perspectives dominating Western debate. For Chinese authors, the new technology presents neither the weaker nor the stronger side with an unequivocal advantage. The new domain's low barriers to entry, the more limited vulnerability of weak actors and the feasibility of independent and strategic cyberwarfare are all factors that favour the weak over the strong. Yet only a few actors possess the technological and financial resources that are a precondition to develop effective cyber weapons. Thus, the new technology's impact on international order appears

[68] Tian, Zhang and Jiang, 'Wangluo Zhan', 104.

[69] Ning and Dan, 'Mao Zedong', 67-8.

[70] Peng Hongqi, 'Qiantan Xinxihua Tiaojian Xia de Yi Lie Sheng You' ('On Defeating the Superior from a Position of Inferiority under Information Conditions'), *Zhongguo Junshi Kexue* 21/1 (2008), 142-48, 147.

URL: http://mc.manuscriptcentral.com/fjss
For Peer Review Only

to be more complicated than often assumed in Western debate. On the one hand, cyberwarfare will not trigger the power diffusion envisaged in the weapon of the weak discourse. On the other hand, contrary to what the weapon of the strong discourse may suggest, it will not result in a consolidation of the existing power hierarchy. Rather, the impact of cyberwarfare on the future of international politics will depend on how weak and strong actors confront the challenges and seize the opportunities that the new technology creates for all.

When it comes to the implications for China's national security, cyberspace is perceived as an intrinsically ambivalent domain. Owing to its persistent technological inferiority, China remains at a disadvantage *vis-à-vis* its stronger rivals: in particular, the United States continues to have the advantage in the new domain, as it does in the traditional ones. Cyberspace is presented in *Guofang Keji* as dominated by U.S. political and cultural threats to China, with Washington leveraging the new technology to advance its traditional agenda of political interference. At the same time, however, the cyber domain also creates new opportunities for China in its military competition with the U.S. Although still in a condition of overall inferiority, Beijing can gain local superiority within the context of a specific cyber conflict. If this goal is achieved, the new technology will dramatically increase China's room for manoeuvre, because of both the U.S. military's and society's greater vulnerability to cyberattacks. Thus, cyber weapons are theorised in *Guofang Keji* as an assassin's mace and cyber campaigns as a key component of any future asymmetric struggle against the superpower.

The perceived ambivalence of cyberspace emerging from *Guofang Keji* is reflected in two main directions of Beijing's current strategy toward the new domain. First, China is expanding its military capabilities by developing new doctrinal principles and consolidating its cyber forces. In the 2013 edition of the *Science of Military Strategy*, the PLA Academy of Military Sciences presented cyberspace not only as the arena of a new 'military struggle' where China 'remains on the whole at disadvantage', but also as a critical domain for 'gaining the war initiative' (*duoqu zhanzheng zhudongquan*) against a stronger enemy.[71] An offensive approach (*yi gong wei zhu*) to cyberspace was accordingly prescribed, with attacks on both the enemy's software and hardware. Based on the principle of 'peace-war combination, civil-military integration', it was recommended that 'civilians are used to cover the military' (*yi min yan jun*) in peacetime and that 'the military and civilians join hands' (*jun min lianshou*) to attack the enemy in wartime.[72] The establishment of the PLASSF in late

[71] Junshi Kexueyuan Junshi Zhanlüe Yanjiubu (Academy of Military Sciences Military Strategy Research Institute), *Zhanlüe Xue* (*The Science of Military Strategy*) (Beijing: Junshi Kexue Chubanshe 2013), 130-31, 196.

[72] *Ibid*., 131. This emphasis on 'peace-war combination' is coherent with the orthodox Marxist-Leninist view of war as the continuation of peacetime political struggle. In Mao's words, 'politics is war without bloodshed while war is politics with bloodshed', or even more explicitly: 'war is the continuation of politics, i.e. the continuation of peace'. See Zhang

URL: http://mc.manuscriptcentral.com/fjss
For Peer Review Only

2015 was an organizational response to these doctrinal developments. In the previous decade, a major obstacle to advancements in China's cyberwarfare capabilities had been the compartmentalization of responsibilities among separate PLA institutions, including the General Staff's Third and Fourth Departments (3PLA, 4PLA), respectively in charge of technical reconnaissance and electronic countermeasures.[73] Under the 2015 reform, the newly-established PLASSF Network Systems Department has been given authority over both the cyber espionage forces previously under the 3PLA and the computer network attack forces previously under the 4PLA.[74]

Second, China is trying to reduce its reliance on foreign technology, which is identified as a major source of vulnerability for the military and the country as a whole. This issue figured prominently in Xi Jinping's important speech at the 2016 Cybersecurity and Informatization Work Conference. According to Xi, the 'greatest hidden danger' that China faces in the cyber domain lies in the persistent control exercised by others over 'Internet's core technologies' (*hulianwang hexin jishu*), i.e. 'basic technology, or common technology', 'asymmetric technology, or "assassin's mace" technology' (*shashoujian jishu*), and 'advanced technology, or disruptive technology'.[75] To make progress in this area, Xi called for a balanced approach that 'correctly handles the relationship between opening and autonomy'. On the one hand, China should continue to cooperate with technologically advanced countries, welcoming their companies to invest in China. On the other hand, such cooperative projects should be used to advance China's own technological capabilities, with the ultimate goal of 'autonomous innovation'.[76] In order to reduce reliance on foreign technology, China

---

Yining et al., *Zhongguo Xiandai Junshi Sixiang* (*China's Contemporary Military Thought*) (Beijing: Guofang Daxue Chubanshe 2006), 75-9, 109-12. Of course, this view is in turn coherent with Clausewitz's: on the affinity between the Marxist-Leninist tradition and Clausewitz's teachings, see Jacob W. Kipp, 'Lenin and Clausewitz: The Militarization of Marxism, 1914-1921', *Military Affairs* 49/4 (1985), 184-91; Azar Gat, 'Clausewitz and the Marxists: Yet Another Look', *Journal of Contemporary History* 27/2 (1992), 363-82.

[73] Stokes, 'The Chinese People's Liberation Army Computer Network Operations Infrastructure'; Costello and McReynolds, *China's Strategic Support Force*, 8; Kania and Costello, 'The Strategic Support Force and the Future of Chinese Information Operations'.

[74] Burton and Stokes, *The People's Liberation Army Strategic Support Force*, 9; Costello and McReynolds, *China's Strategic Support Force*, 25.

[75] Xi Jinping, 'Zai Wangluo Anquan he Xinxihua Gongzuo Zuotanhui shang de Jianghua' (Speech at the Cybersecurity and Informatization Work Conference), *Renmin Ribao*, 26 April 2016, 1.

[76] On the apparent contradiction between cooperation and self-reliance in China's industrial policies see Greg Austin, *Cybersecurity in China. The Next Wave* (Cham: Springer 2018), 41-64. On autonomous innovation in China's cybersecurity sector see Tai Ming Cheung, 'The Rise of China as a Cybersecurity Industrial Power. Balancing National Security, Geopolitical, and Development Priorities', *Journal of Cyber Policy* 3/3 (2018), 306-26. On autonomous

For Peer Review Only

is increasingly focusing on integration between the military industrial base, civilian state-owned enterprises, and the private sector, under the so-called 'civil-military fusion' (*jun min ronghe*) concept. In this respect, an important role is played by the PLASSF itself, which is reportedly developing cooperative research projects with civilian universities and private companies.[77]

While these developments are a reason for growing concern in the United States,[78] what our analysis of *Guofang Keji* suggests is that Chinese analysts remain cautious about China's prospects in the cyber competition. The ambivalent impact of cyberspace on China's national security is in fact amplified by the changing place that China itself occupies within the new domain. As emphasised in several *Guofang Keji* articles, protracted economic and social development is rapidly transforming China from a weak and underdeveloped country into an established economic and military power. When it comes to cyberwarfare, the implications of such a transformation are twofold. On the one hand, China's economic rise is creating a solid base for the development of advanced cyberwarfare capabilities. In a flourishing economy, the government has more resources to invest in military modernisation programmes, which can also benefit from the technological progress made in the private sector, as well recognized by Beijing. More broadly, economic growth helps the military to raise the comprehensive level of its technological sophistication, which, in turn, is a precondition for the development of a true cyber assassin's mace. While remaining at a disadvantage *vis-à-vis* the United States, an economically and technologically more advanced China will then be able to wage cyberwarfare more effectively against its stronger rival.

On the other hand, however, development is making China more and more dependent on networks – and, therefore, more exposed to cyberattacks. This is the case with China's military, whose modernisation process has now moved from the stage of 'mechanisation' to that of 'informatisation', with a shift in the 'mode of generating combat effectiveness'.[79] Western scholars have long expected

---

innovation in the broader context of China's defence technology see Tai Ming Cheung, 'Innovation in China's Defense Technology Base: Foreign Technology and Military Capabilities', *Journal of Strategic Studies* 39/5-6 (2016), 728-61.

[77] On 'civil-military fusion' see Daniel Alderman *et al*., 'The Rise of Chinese Civil-Military Integration', in Tai Ming Cheung (ed.), *Forging China's Military Might. A New Framework for Assessing Innovation* (Baltimore: Johns Hopkins University Press 2014), 109-35. On the role of the PLASSF in civil-military fusion see Joel Wuthnow and Phillip C. Saunders, *Chinese Military Reforms in the Age of Xi Jinping: Drivers, Challenges, and Implications* (Washington, D.C.: National Defense University Press 2017), 35-7; Lorand Laskai, 'Civil-Military Fusion and the PLA's Pursuit of Dominance in Emerging Technologies', *China Brief* 18/6 (2018), 12-6.

[78] Department of Defense, *Annual Report to Congress. Military and Security Developments Involving the People's Liberation of China 2018* (Washington, D.C. 2018), 39-41, 60-1, 74-5; Defense Intelligence Agency, *China Military Power. Modernizing a Force to Fight and Win* (Washington, D.C. 2019), 45-6, 97.

[79] Junshi Kexueyuan Junshi Zhanlüe Yanjiubu, *Zhanlüe Xue*, 267-72.

URL: http://mc.manuscriptcentral.com/fjss
For Peer Review Only

such a transformation to undermine 'the asymmetry of vulnerability' between the PLA and its rivals, thus ironically making the former less secure than it had been in the past.[80] Chinese authors seem to be well aware of this challenge and openly warn that Internet dependency is, in fact, creating new 'weak points that are vulnerable to attacks'.[81] Because of the increasing role of informatisation in everyday life, however, it is not just the PLA but the whole of China's society that is becoming more vulnerable. As a result, China itself is now exposed to the 'information and infrastructure warfare' theorised in *Guofang Keji* against a stronger enemy. Hence, the ambivalent impact of the new domain on China's security: the same process that is making China better prepared to 'defeat the superior from a position of inferiority' is simultaneously creating new vulnerabilities that could be easily exploited by the U.S., whose hegemony over cyberspace remains largely unchallenged.

For Peer Review Only

[80] Lindsay, 'The Impact of China', 35; see also Inkster, *China's Cyber Power*, 97, 148.

[81] Cheng, Zhang and Chang, 'Wangluo Kongjian', 82; see also Wu, 'Jiakuai Zhongguo'.

Bibliography

Adamsky, Dmitry (Dima), 'From Moscow With Coercion: Russian Deterrence Theory and Strategic Culture', *Journal of Strategic Studies* 41/1-2 (2018), 33-60.

Alderman, Daniel, Lisa Crawford, Brian Lafferty and Aaron Shraberg, 'The Rise of Chinese Civil-Military Integration', in Tai Ming Cheung (ed.), *Forging China's Military Might. A New Framework for Assessing Innovation* (Baltimore: Johns Hopkins University Press 2014), 109-35.

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

Allison, Graham, 'The Thucydides Trap: Are the U.S. and China Headed for War?', *The Atlantic* (September 24, 2015), https://www.theatlantic.com/international/archive/2015/09/united-states-china-war-thucydides-trap/406756/.

Andres, Richard B., 'The Emerging Structure of Strategic Cyber Offense, Cyber Defense, and Cyber Deterrence', in Derek S. Reveron (ed.), *Cyberspace and National Security. Threats, Opportunities, and Power in a Virtual World* (Washington, DC: Georgetown U.P., 2012), 89-104.

Arquilla, John, 'Cyberwar Is Already Upon Us. But Can It Be Controlled?', *Foreign Policy*, February 2012, 27, http://foreignpolicy.com/2012/02/27/cyberwar-is-already-upon-us/#.

Austin, Greg, *Cybersecurity in China. The Next Wave* (Cham: Springer 2018).

Author, 2018.

Betz, David, 'Cyberpower in Strategic Affairs: Neither Unthinkable nor Blessed', *Journal of Strategic Studies* 35/5 (2012), 689-711.

Betz, David J., and Tim Stevens, *Cyberspace and the State. Toward a Strategy for Cyber-Power* (London: IISS 2011).

Blank, Stephen, 'Web War I: Is Europe's First Information War a New Kind of War?', *Comparative Strategy* 27/3 (2008), 227-47.

Blasko, Dennis J., '"Technology Determines Tactics": The Relationship Between Technology and Doctrine in Chinese Military Thinking', *Journal of Strategic Studies* 34/3 (2011), 355-81.

Brenner, Joel, and Jon R. Lindsay, 'Debating the Chinese Cyber Threat', *International Security* 40/1 (2015), 191-95.

Bruzdzinski, Jason, 'Demystifying *Shashoujian*: China's "Assassin's Mace" Concept', in Andrew Scobell and Larry Wortzel (eds.), *Civil-Military Change in China: Elites, Institutes, and Ideas After the 16th Party Congress* (Carlisle, PA: Strategic Studies Institute 2004), 309-64

For Peer Review Only

Bucci, Steven, 'Joining Cybercrime and Cyberterrorism. A Likely Scenario', in Derek S. Reveron (ed.), *Cyberspace and National Security. Threats, Opportunities, and Power in a Virtual World* (Washington, DC: Georgetown U.P. 2012), 57-68.

Burton, Rachel and Mark Stokes, *The People's Liberation Army Strategic Support Force. Leadership and Structure* (Arlington, VA: Project 2049 Institute 2018).

Cai Jun and Yu Xiaohong, 'Meiguo Wangluo Kongjian Zuozhan Nengli Jianshe' ('On the Construction of U.S. Cyberspace Operations Capabilities), *Guofang Keji* 39/3 (2018), 105-9.

Chen Tian, Xian Ming and Li Zili, 'Mei Jun Wangluo Kongjian Zuozhan Guihua Yanjiu' ('Research on the Planning of U.S. Cyber Warfare'), *Guofang Keji* 37/3 (2016), 68-72.

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

Cheng Shaojie, Zhang Tao and Chang Zhenyu, 'Wangluo Kongjian yu 21 Shiji de "Shouzhan" ' ('Cyberspace and "First Strike" in the Twenty-First Century'), *Guofang Keji* 30/6 (2009), 81-4.

Cheung, Tai Ming, 'Innovation in China's Defense Technology Base: Foreign Technology and Military Capabilities', *Journal of Strategic Studies* 39/5-6 (2016), 728-61.

Cheung, Tai Ming, 'The Rise of China as a Cybersecurity Industrial Power. Balancing National Security, Geopolitical, and Development Priorities', *Journal of Cyber Policy* 3/3 (2018), 306-26.

Choucri, Nazli, *Cyberpolitics in International Relations* (Cambridge, MA: MIT Press 2012).

Costello, John and Joe McReynolds, *China's Strategic Support Force: A Force for a New Era* (Washington, D.C.: National Defense University Press 2018).

Defense Intelligence Agency, *China Military Power. Modernizing a Force to Fight and Win* (Washington, D.C. 2019), 45-6, 97.

Demchak, Chris C., *Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security* (Athens, GA: University of Georgia Press 2011).

Deng Feng, 'Bianzheng Renshi Gao Jishu Zhanzheng Zhong Yi Lie Sheng You de Wenti' ('Dialectical Understanding of the Issue of Defeating the Superior from a Position of Inferiority in High-Tech Wars'), *Zhongguo Junshi Kexue* 17/3 (2004), 107-11.

Department of Defense, *Annual Report to Congress. Military and Security Developments Involving the People's Liberation of China 2018* (Washington, D.C. 2018), 39-41, 60-1, 74-5.

Du Yanyun and Liu Yangyue, 'Zhong Mei Wangluo Kongjian Boyi yu Jingzheng' ('Sino-U.S. Game and Competition in Cyberspace') *Guofang Keji* 35/3 (2014), 70-82.

For Peer Review Only

Eriksson, Johan, and Giampiero Giacomello, 'Conclusion. Digital-Age Security in Theory and Practice', in Johan Erkisson and Giampiero Giacomello (eds.), *International Relations and Security in the Digital Age* (London: Routledge 2007), 173-84.

Eriksson, Johan, and Giampiero Giacomello (eds.), *International Relations and Security in the Digital Age* (London: Routledge 2007).

Farwell, James P., and Rafal Rohozinski, 'Stuxnet and the Future of Cyber War', *Survival* 53/1 (2011), 23-40.

Fu Yanhong and Zhao Yang, 'Wangluo Kongjian Junbei Kongzhi Yanjiu Xianzhuang ji Qishi Sikao ('State of Research on Cyberspace Arms Control and Assessment'), *Guofang Keji* 34/1 (2013), 34-7.

Gartzke, Erik, 'The Myth of Cyberwar. Bringing War in Cyberspace back down to Earth', *International Security* 38/2 (2013), 41-73.

Gat, Azar, 'Clausewitz and the Marxists: Yet Another Look', *Journal of Contemporary History* 27/2 (1992), 363-82.

Giacomello, Giampiero, 'Bangs for the Buck: A Cost-Benefit Analysis of Cyberterrorism', *Studies in Conflict & Terrorism* 27/5 (2004), 387-408.

Goh, Evelyn, 'Great Powers and Hierarchical Order in Southeast Asia: Analyzing Regional Security Strategies', *International Security* 32/3 (2008), 113-57.

Gompert, David C., and Martin Libicki, 'Waging Cyber War the American Way', *Survival* 57/4 (2015), 7-28.

Guo Fuliang, Yang Xinde and Zhou Gang, 'Wai Jun Wangluo Zhan Fazhan Xiankuang Yanjiu ji Qishi' ('Analysis and Assessment of the Current Situation of Cyberwar Development in Foreign Armed Forces'), *Guofang Keji* 34/3 (2013), 49-52.

Gvosdev, Nikolas K., 'The Bear Goes Digital. Russia and Its Cyber Capabilities', in Derek S. Reveron (ed.), *Cyberspace and National Security. Threats, Opportunities, and Power in a Virtual World* (Washington, DC: Georgetown U.P., 2012), 173-89.

Holmes, James R., 'Beware the "Thucydides Trap" Trap. Why the U.S. and China Aren't Necessarily Athens and Sparta or Britain and Germany before WWI', *The Diplomat* (June 13, 2013), https://thediplomat.com/2013/06/beware-the-thucydides-trap-trap/

Hu Yanjing and Zhan Zhongkun, 'Jiakuai Tuijin Xinxi Gongfang Xinxing Zuozhan Liliang Jianshe' ('On Speeding Up the Construction of New Combat Force of Information Attack and Defence'), *Guofang Keji* 38/2 (2017), 64-7.

Huang Renquan and Li Weimin, 'Kongfang Duikang Zhanchang Tuozhan Dao Wang Dian Kongjian dui Weilai Guojia Fangkong de Yingxiang' ('The Extension of the Air Defence Battlefield to

For Peer Review Only

Cyberspace: Impact on the Future of National Antiaircraft Defence'), *Guofang Keji* 33/3 (2012), 46-50.

Huo Jiajia, 'Meiguo Wangluo Fangwu Chengbao de Xianzhuang' ('State of Cyber Defence Contracting in the United States'), *Guofang Keji* 37/6 (2016), 100-03.

Ikenberry, G. John, 'Between the Eagle and the Dragon: America, China, and Middle State Strategies in East Asia', *Political Science Quarterly* 131/1 (2016), 9-43.

Inkster, Nigel, *China's Cyber Power* (London: Adelphi Series 2015).

Jiang Lei, *Xiandai Yi Lie Sheng You Zhanlüe* (Contemporary Strategy for Defeating the Superior from a Position of Inferiority) (Beijing: Guofang Daxue Chubanshe 1997).

Johnston, Alastair Iain, *Cultural Realism. Strategic Culture and Grand Strategy in Chinese History* (Princeton, N.J.: Princeton U.P. 1995).

Junshi Kexueyuan Junshi Zhanlüe Yanjiubu (Academy of Military Sciences Military Strategy Research Institute), *Zhanlüe Xue* (*The Science of Military Strategy*) (Beijing: Junshi Kexue Chubanshe 2013).

Junshi Kexueyuan Zhanlüe Yanjiubu (Academy of Military Sciences Strategy Research Institute), *Zhanlüe Xue* (*The Science of Military Strategy*) (Beijing: Junshi Kexue Chubanshe 2001).

Kang, David C., *China Rising. Peace, Power, and Order in East Asia* (New York, NY: Columbia U.P. 2007).

Kania, Elsa B. and John K. Costello, 'The Strategic Support Force and the Future of Chinese Information Operations', *The Cyber Defense Review* 3/2 (2018), 105-21.

Ke Hongfa, Zhu Jilu and Zhao Rong, 'Tuijin Wangluo Kongjian Hexin Zhiyuan Nengli Jianshe' ('Promoting the Building-Up of Core Supporting Capabilities in Cyberspace'), *Guofang Keji* 38/2 (2017), 50-4.

Kello, Lucas, 'The Meaning of the Cyber Revolution. Perils to Theory and Statecraft', *International Security* 38/2 (2013), 7-40.

Kipp, Jacob W., 'Lenin and Clausewitz: The Militarization of Marxism, 1914-1921', *Military Affairs* 49/4 (1985), 184-91.

Klimburg, Alexander, 'Mobilizing Cyber Power', *Survival* 53/1 (2011), 41-60.

Koblentz, Gregory D., and Brian M. Mazanec, 'Viral Warfare: The Security Implications of Cyber and Biological Weapons', *Comparative Strategy* 32/5 (2013), 418-34.

Kremer, Jan-Frederik, and Benedikt Müller (eds.), *Cyberspace and International Relations. Theory, Prospects and Challenges* (Belin: Springer 2014).

For Peer Review Only

Kugler, Richard R., 'Deterrence of Cyber Attacks', in Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz (eds.), *Cyberpower and National Security* (Washington, DC: National Defense U.P. 2009), 309-40.

Laskai, Lorand, 'Civil-Military Fusion and the PLA's Pursuit of Dominance in Emerging Technologies', *China Brief* 18/6 (2018), 12-6.

Liang Meng, Han Yue and Qiao Zheng, 'Meiguo "Guofangbu Wangluo Kongjian Zuozhan Zhanlüe" Shuping' ('A Discussion of the U.S. "Department of Defense Strategy for Operating in Cyberspace" '), *Guofang Keji* 33/1 (2012), 84-7.

Libicki, Martin C., *Conquest in Cyberspace. National Security and Information Warfare* (Cambridge: Cambridge U.P. 2007).

Libicki, Martin C., *Cyberdeterrence and Cyberwar* (Santa Monica: RAND 2009).

Lieberthal, Kenneth, and Peter W. Singer, *Cybersecurity and U.S.-China Relations* (Washington, DC: Brookings, 2012).

Liff, Adam P., 'Cyberwar: A New "Absolute Weapon"? The Proliferation of Cyberwarfare Capabilities and Interstate War', *Journal of Strategic Studies* 35/3 (2012), 401-28.

Liff, Adam P., 'Whither the Balancers? The Case for a Methodological Reset', *Security Studies* 25/3 (2016), 420-59.

Lin, Ying Yu, 'One Step Forward, One Step Back for PLA Military Education', *China Brief* 18/7 (2018), https://jamestown.org/program/one-step-forward-one-step-back-for-pla-military-education/.

Lindsay, Jon R., 'Stuxnet and the Limits of Cyber Warfare', *Security Studies* 22/3 (2013), 365-404.

Lindsay, Jon R., 'The Impact of China on Cybersecurity. Fiction and Friction', *International Security* 39/3 (2015), 7-47.

Lindsay, Jon R., Tai Ming Cheung and Derek S. Reveron (eds.), *China and Cybersecurity. Espionage, Strategy, and Politics in the Digital Domain* (Oxford: Oxford U.P. 2015).

Liu Yangyue, 'Jun Min Ronghe Shijiao Xia de Meiguo Wangluo Anquan Rencai Zhanlüe' ('U.S. Strategy for Cybersecurity Personnel From the Point of View of Civil-Military Fusion'), *Guofang Keji* 39/1 (2018), 71-5.

Ma Zengjun and Li Jian, 'Mei Jun Wangluo Zuozhan Zhihui yu Kongzhi de Guoqu, Xianzai yu Jianglai' ('Past, Present and Future of the U.S. Cyberwarfare Command and Control'), *Guofang Keji* 35/5 (2014), 73-85.

Manson, George P. III, 'Cyberwar: The United States and China Prepare for the Next Generation of Conflict', *Comparative Strategy* 30/2 (2011), 121-33.

For Peer Review Only

McGraw, Gary, 'Cyber War is Inevitable (Unless We Build Security In)', *Journal of Strategic Studies* 36/1 (2013), 109-19.

Moore, Gregory J., 'Avoiding a Thucydides Trap in Sino-American Relations (… and 7 Reasons Why that Might be Difficult)', *Asian Security* 13/2 (2017), 98-115.

Newmyer, Jacqueline, 'The Revolution in Military Affairs with Chinese Characteristics', *Journal of Strategic Studies* 33/4 (2010), 483-504.

Ning Jun and Dan Xiufa, 'Mao Zedong Yi Ruo Sheng Qiang Lilun Zai Yanjiu' ('New Research on Mao Zedong's Theory of the Defeating the Strong from a Position of Weakness'), *Zhongguo Junshi Kexue* 23/3 (2010), 60-70.

Nye, Joseph S., 'Nuclear Lessons for Cyber Security?', *Strategic Studies Quarterly* 5/4 (2011), 18-38.

Nye, Joseph S., *The Future of Power* (New York: Public Affairs 2011).

Peng Hongqi, 'Qiantan Xinxihua Tiaojian Xia de Yi Lie Sheng You' ('On Defeating the Superior from a Position of Inferiority under Information Conditions'), *Zhongguo Junshi Kexue* 21/1 (2008), 142-48.

Peterson, Dale, 'Offensive Cyber Weapons: Construction, Development, and Employment', *Journal of Strategic Studies* 36/1 (2013), 120-24.

Pollpeter, Kevin, '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* (Oxford: Oxford U.P. 2015), 138-62.

Pollpeter, Kevin L., Michael S. Chase and Eric Heginbotham, *The Creation of the PLA Strategic Support Force and Its Implications for Chinese Military Space Operations* (Santa Monica, CA: RAND Corporation 2017).

Rattray, Greg, *Strategic Warfare in Cyberspace* (Cambridge, MA: MIT Press 2001).

Reveron, Derek, 'An Introduction to National Security and Cyberspace', in Derek S. Reveron (ed.), *Cyberspace and National Security. Threats, Opportunities, and Power in a Virtual World* (Washington, DC: Georgetown U.P., 2012), 3-19.

Rid, Thomas, *Cyber War Will Not Take Place* (London: Hurst & Company 2013).

Rid, Thomas, and Ben Buchanan, 'Attributing Cyber Attacks', *Journal of Strategic Studies* 38/1-2 (2015), 4-37.

Ross, Robert S., 'Balance of Power Politics and the Rise of China: Accommodation and Balancing in East Asia', *Security Studies* 15/3 (2006), 355-95.

Ross, Robert S. and Øystein Tunsjø (eds.), *Strategic Adjustment and the Rise of China. Power and Politics in East Asia* (Ithaca, NY: Cornell U.P. 2017).

For Peer Review Only

Segal, Adam, 'Chinese Computer Games: Keeping Safe in Cyberspace', *Foreign Affairs* 91/2 (2012), 14-20.

Shang Liang, Yang Guoxin, Shi Jinlai and Sui Shilong, 'Wangluo Zhan Budui. Ge Guo Jun Zhong Xin Chong' ('Cyberwar Forces: The New Favourite of Every Country's Military'), *Guofang Keji* 30/4 (2009), 89-92.

Sharp, Travis, 'Theorizing Cyber Coercion: The 2014 North Korean Operation Against Sony', *Journal of Strategic Studies* 40/7 (2017), 898-926.

Sheldon, Robert, and Joe McReynolds, 'Civil-Military Integration and Cybersecurity. A Study of Chinese Information Warfare Militias', in Jon R. Lindsay, Tai Ming Cheung and Derek S. Reveron (eds.), *China and Cybersecurity. Espionage, Strategy, and Politics in the Digital Domain* (Oxford: Oxford U.P. 2015), 188-222.

Shen Xueshi, 'Wangluo Kongjian Gong Fang Jishu Fazhan Dongxiang Fenxi' ('An Analysis of the Development Trends in Cyberspace Offence and Defence Technology'), *Guofang Keji* 38/4 (2017), 42-6.

Slayton, Rebecca, 'What Is the Cyber Offense-Defense Balance?: Conceptions, Causes, and Assessment', *International Security* 41/3 (2016/17), 72-109.

Smeets, Max, 'A Matter of Time: On the Transitory Nature of Cyberweapons', *Journal of Strategic Studies* 41/1-2 (2018), 6-32.

Stokes, Mark A., 'The Chinese People's Liberation Army Computer Network Operations Infrastructure', in Jon R. Lindsay, Tai Ming Cheung and Derek S. Reveron (eds.), *China and Cybersecurity. Espionage, Strategy, and Politics in the Digital Domain* (Oxford: Oxford U.P. 2015), 163-87.

Sun Qiangyin, 'Zhunque Tangxun Xinxihua Zhanzheng Yi Lie Sheng You Zhisheng Jili' ('Exploring the Mechanism of Defeating the Superior from a Position of Inferiority in Informationized War'), *Guofang Keji* 36/1 (2015), 75-8.

Sun Wei, 'Quanli Zhengzhi Shijiao Xia Wangluo Zhuquan de Jichu' ('The Basis of Cyber Sovereignty from the Perspective of Power Politics'), *Guofang Keji* 37/6 (2016), 81-7.

Sun Wei and Bao Chuang, 'Guoji Wangluo Anquan Chanpin Shichang Fazhan Xianzhuang yu Qushi' ('State of Development and Trends of the International Market for Cybersecurity Products'), *Guofang Keji* 37/2 (2016), 59-64.

Tang Lu, 'Qianxi Yi Falü Xingshi Kongzhi Wangluo Junbei Jingsai de Biyaoxing' ('An Analysis on the Necessity of Controlling Cyber Arms Race through Law'), *Guofang Keji* 31/3 (2010), 33-6.

For Peer Review Only

Thomas, Timothy L., 'Google Confronts China's "Three Warfares"', *Parameters* 40/2 (2010), 101-13.

Thomas, Timothy L., 'Nation-State Cyber Strategies: Examples from China and Russia', in Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz (eds.), *Cyberpower and National Security* (Washington, DC: National Defense U.P. 2009), 465-88.

Tian Chengxin, Zhang Feng and Jiang Fei, 'Wangluo Zhan dui Zuozhan de Yingxiang ji Duice' ('Influence of Cyberwarfare on Operations and Countermeasures'), *Guofang Keji* 35/5 (2014), 103-05.

Wang Zengzhuo and Zhu Yajie, 'Mei Jun Wangluo Silingbu yu Guojia Anquan Ju Chaifen de Kenengxing' ('On the Possibility of a Split between the U.S. Cyber Command and the National Security Agency'), *Guofang Keji* 39/5 (2018), 91-6.

Wenger, Andreas, (ed.), "The Internet and the Changing Face of International Relations and Security", special issue, *Information & Security* 7 (2001).

Whyte, Christopher, 'Ending Cyber Coercion: Computer Network Attack, Exploitation and the Case of North Korea', *Comparative Strategy* 35/2 (2016), 93-102.

Wu Chenggang, 'Jiakuai Zhongguo "Wangluo Guofang" Jianshe de Zhanlüe Sikao' ('Strategic Reflection on Accelerating the Construction of China's "Cyber National Defence" '), *Guofang Keji* 33/3 (2012), 1-4.

Wu Tong, 'Jingwai Xinxi Wangluo Jiankong Xingshi yu Tiaozhan' ('Situation and Challenges of Information Network Monitoring Abroad'), *Guofang Keji* 37/3 (2016), 40-3.

Wu Zecheng, 'Meiguo Wangluo Baquan dui Zhongguo Guojia Anquan de Yingxiang ji Duice' ('The Influence of U.S. Cyber Hegemony on China's National Security and Countermeasures against It'), *Guofang Keji* 35/1 (2014), 55-60.

Wuthnow, Joel, and Phillip C. Saunders, *Chinese Military Reforms in the Age of Xi Jinping: Drivers, Challenges, and Implications* (Washington, D.C.: National Defense University Press 2017), 35-7.

Xi Jinping, 'Zai Wangluo Anquan he Xinxihua Gongzuo Zuotanhui shang de Jianghua' (Speech at the Cybersecurity and Informatization Work Conference), *Renmin Ribao*, 26 April 2016, 1.

Xiao Xunlong and Li Shouqi, 'Wangluo Yulun Zhan de Lilun Tanxi' ('Theoretical Analysis of Cyber Public Opinion Warfare'), *Guofang Keji* 35/2 (2014), 5-8.

Yang Tengfei, Zhu Yaohua and Zhang Weichao, 'Heping Shiqi Wangluo Yulun Zhan de Tedian ji Duice Chuyi' ('Observations on the Characteristics of and Countermeasures to Cyber Public Opinion Warfare in Peacetime'), *Guofang Keji* 35/2 (2014), 33-6.

For Peer Review Only

Ye Zheng, 'From Cyberwarfare to Cybersecurity in the Asia-Pacific and Beyond', in Jon R. Lindsay, Tai Ming Cheung and Derek S. Reveron (eds.), *China and Cybersecurity. Espionage, Strategy, and Politics in the Digital Domain* (Oxford: Oxford U.P. 2015), 123-37.

Zhan Xiaosu, 'Jiaqiang Wangluo Guofang Jianshe Zhanlüe Yunchou Xuyao Qianghua de Liu Zhong Yishi' ('On the Six Elements of Awareness that Should Be Strengthened in order to Reinforce the Strategic Planning for Cyber National Defence Construction'), *Guofang Keji* 34/6 (2013), 69-72.

Zhang Jianchao, Shen Xueshi and Zhong Hua, 'Mei Jun Wangluo Kongjian Zuozhan Lilun Fazhan ji Yingxiang Fenxi' ('Analysis of the Impact and Development of the U.S. Military Cyberspace Operations Theory'), *Guofang Keji* 37/3 (2016), 63-7.

Zhang Yining, Xu Yan, Sun Kejia and Zhang Wenjie, *Zhongguo Xiandai Junshi Sixiang* (China's Contemporary Military Thought) (Beijing: Guofang Daxue Chubanshe 2006).

Zheng Hebin, 'Wangluo Junbei dui Zhuquan de Yingxiang ji Woguo Duice' ('The Impact of Cyber Arms on Sovereignty and Countermeasures of China), *Guofang Keji* 34/2 (2013), 62-8.

Zhongguo Da Baike Quanshu – Junshi Bianweihui (Editorial Committee of 'Chinese Encyclopedia – Military'), *Zhongguo Da Baike Quanshu – Junshi* (*Chinese Encyclopedia – Military*) (Beijing: Zhongguo Da Baike Quanshu Chubanshe 2005).

Zhonghua Renmin Gongheguo Guowuyuan Xinwen Bangongshi (Information Office of the PRC State Council), *Zhongguo de Junshi Zhanlüe* (China's Military Strategy) (Beijing: Renmin Chubanshe 2015).

Zhuang Lin and Si Huijing, 'Meiguo Wangluo Anquan Zhanlüe de Shizhi' ('Essence of the U.S. Cybersecurity Strategy'), *Guofang Keji* 34/4 (2013), 74-8.

For Peer Review Only