Chinese Journal of International Review
Vol. 1, No. 2 (2019) 1950002 (23 pages)

DOI: 10.1142/S2630531319500021

From Offense Dominance to Deterrence: China's Evolving Strategic Thinking on Cyberwar

Tianjiao Jiang
School of International Relations and Public Affairs
Shanghai International Studies University, P. R. China
jiangtj09@outlook.com

Published 2 August 2019

Abstract

This paper examines China's strategic thinking on cyberwar. It has been widely argued that the People's Liberation Army (PLA) has shown strong interest in launching large-scale cyberattacks against the US during warfare or peacetime. However, such views ignore the fact that the PLA must restrain itself due to the uncertainties of cyberattack, such as collateral damage, blowback, and escalation. In fact, Chinese experts follow US perceptions and cyberwar practices very closely, which has contributed to Beijing's evolving strategic thinking over the past decades. From the 1990s to early 2000s, the "ideology of offense" was the PLA's primary approach to the "informationization leaping forward". Due to the shock of the Gulf War, most of the military strategists advocated cyber offense in order to catch up with the new round of revolution in military affairs. However, after 2008, both military and civilian experts started to increasingly question the effectiveness of cyberattack after studying their peers' criticism against cyber deterrence in the US. There was no consensus on national cybersecurity strategy until 2015 when there was a call for China to develop a cyber deterrence strategy as a reaction to the further development of cyber deterrence by the US. The latest Chinese official documents on cybersecurity have reflected the shift of its strategic thinking.

Keywords

Cyberwar; cyber deterrence; China's cybersecurity strategy.

1. Introduction

There have been many discussions on how China takes advantage of cyber technology as a strategic tool to increase its power. The well-publicized disputes on cyber espionage between China and the US have raised further questions about how Beijing will use cyber capabilities in future conflicts or if the Chinese would even use them in a coercive manner, which poses a more significant threat to Washington. On the one hand, a high level dependency on cyber systems makes the socio-economic development of the US extremely vulnerable (The Economist, 2017). On the other hand, cyberwar is perceived as increasingly likely due to "its effectiveness as a weapon; the relative low cost of entry; the appeal as an asymmetric form of warfare; the lack of clearly defined international constraints; and difficulty of deterrence" (Mazanec and Thayer, 2015a). And China is believed to have made long-term preparations for this kind of cyberwar against the US (U.S.–China Economic and Security Review Commission, 2017).

Observers have expressed serious concerns over the scenario of the People's Liberation Army (PLA) launching a cyberwar against the US. However, there has been no sign of any large-scale cyberattack, except for continuous back and forth disputes about cyber espionage across the Pacific. The argument that a cyberwar between China and the US is unavoidable is internally contradictory. It ignores the fact that the PLA must restrain itself due to the uncertainties of cyberattack such as collateral damage, blowback, and escalation. But such restraint does not come by nature. I argue that China has gone through three stages of understanding on cyberwar: from the 1990s to 2008, from 2009 to 2014, and from 2015 to present. The first stage witnessed the PLA's "informatization leap forward" when most military strategists advocated cyber offense due to the shock of the Gulf War. But the English literature largely missed the domestic debate on the effectiveness of cyberattack after 2008 and the shaping of cybersecurity strategy in recent years. In fact, the concept and practice of cyberwar raised by the US have strong influence on Chinese strategists and policy advisers. It is worthwhile to examine how they borrow ideas, translate key words, and quote arguments from the US experts during domestic debates. It may also shed light on how the input from academia and think tanks will decide the policy-making of China's cybersecurity strategy.

In my analysis, I combine the research from both military and non-military sources to illustrate the vibrant debate on China's strategic thinking about

cyberwar. Despite a lack of official military doctrine on cyberwarfare, there have been many textbooks and research papers discussing the PLA's understanding of cyberwar. Additionally, the viewpoints from the civilian strategists and think tanks can never be undervalued due to Beijing's continuing reform of the decision-making system. In fact, it is not the PLA, but the Leading Small Group (LSG) for Cybersecurity and Informatization that coordinates different departments and makes cybersecurity policy (Inkster, 2016; see footnote 1).[1] With President Xi's call to develop "a new type of think tank with Chinese characteristics", think tanks are playing important roles in policy-making through their channels to the government (Glaser and Saunders, 2002; see footnote 2).[2] Besides think tanks, Chinese leaders also receive advice from scholars at top universities, including Peking University, Tsinghua University, Fudan University, Renmin University, and East China University of Political Science and Law.[3] Think tanks and university scholars usually apply for research projects sponsored by the government in order to submit internal reports or publish open journals to influence policy-making.[4] As internal reports are rarely declassified, the openly published academic papers are the best resources available from which one can summarize policy debate issues and predict

[1] For the background of LSG in China's decision-making see Miller (2014).

[2] "CCP General Office and State Council General Office Opinions Concerning Strengthening the Construction of New Types of Think Tanks With Chinese Characteristics," translated by China Copyright and Media, https://chinacopyrightandmedia.wordpress.com/2015/01/20/ccp-general-office-and-state-council-general-office-opinions-concerning-strengthening-the-construction-of-new-types-of-think-tanks-with-chinese-characteristics/, Accessed on June 15, 2017. The contribution of the Chinese Academy of Social Sciences (CASS) to the reform and opening up policy during the 1980s has been well studied by many Western scholars. (See Macfarquhar (2011)). In foreign affairs, the China Institute of International Studies (CIIS) directed by Ministry of Foreign Affairs, the China Institutes of Contemporary International Relations (CICIR) directed by Ministry of State Security and the Shanghai Institute for International Studies (SIIS) directed by Shanghai Foreign Affairs Office are very influential even according to the global think tanks ranking system. (See McGann (2017) and also see Shambaugh (2002)).

[3] For example, Wang Huning, former director of department of international relations at Fudan, has served as policy adviser of three-generation leadership and is now Director of the Policy Research Office of the CCP's Central Committee. (See Li (2009)).

[4] For example, 'the General Office of the CASS periodically submits two versions of the internal CASS Important Report (Yaobao) to the central government and other agencies: Information Special Report (Xinxi zhuanbao) and Leader Reference (lingdaocanyue)'. (See Zhu (2011a,b)).

potential policy shifts. In this research, I turn to academic journals and reports from the civilian side to complement military studies on cyberwar that aim to shed light on Beijing's intentions to develop cyberwar capabilities. All of the papers were selected through the Chinese Social Sciences Citation Index (CSSCI), an authoritative academic journal index widely used in China (see footnote 4). The authors of the sampled articles are mostly professors at prominent universities or analysts at influential think tanks. As the Western audience have not reviewed such a large number of Chinese journals and reports openly discussing China's understanding of cyberwar and cyber deterrence, this paper also aims to fill the literature gap in China's cybersecurity.

This paper only focuses on large-scale computer network attacks (CNAs) between state actors rather than computer network exploitation (CNE) attacks. In the US Department of Defense definition, both CNA and CNE are considered as hostile computer network operations (CNOs) (US Department of Defense, 2011). CNA is the use of computer networks to disrupt, deny, degrade, or destroy either the information resident in enemy computers and computer networks, or the computers and networks themselves, while CNE is usually equal to cyber espionage activities. Although there is a blurred line between CNA and CNE, they can still be separated (Kello, 2013a). This paper defines cyberwar as "hostile actions in cyberspace that have effects that amplify or are equivalent to major kinetic violence" (Nye, 2011a) or "employs CNAs as a use of force to disrupt an opponent's physical infrastructure for political gain" (Lindsay, 2013a). There are basically two kinds of cyberwar: operational cyberwar (acting against military targets during a war) and strategic cyberwar (cyberattacks on enemy civilian infrastructures) (Libicki, 2009).

2. Fallacies on the China–US Cyberwar Scenario

The debate on cyberwar has lasted for many years. The pessimist argues that cyberwar is coming or has already come (Arquilla and Ronfeldt, 1993; McConnell, 2010). The nature of cyber technology is going to change the interactions between states and brings greater instability to the world. Such fear coincides with the relative decline of the US and the rise of China, which makes many China watchers further argue that the PLA has been preparing a major cyberattack on the US for decades. The cyberwar scenario between China and the US has become both the content and driving

force of such fear. However, whether there is a set course of conflict or whether the threat has been exaggerated deserves a more careful examination. Several analysts strongly question such arguments. Rid (2013) argues that cyberwar will never happen. Lindsay (2013b) and Gartzke (2013a) point out that a "digital Pearl Harbor" is unrealistic on both operational and strategic grounds. Dunn-Cavelty (2008) suggests that the growing perceptions of fear among governments and policymakers only exacerbate cyber threats. As both the threats and the opportunities brought by new technology are usually oversold and exaggerated, "confusion and misinformation" have pervaded discussions on cybersecurity (Singer and Friedman, 2014; Betz and Stevens, 2011a).

The pessimistic perspective suggests that the revolution of cyber technology has fundamentally impacted the world military balance and international relations (Clarke and Knake, 2010). The problem of attribution and offense dominance are the main driving factors of such instability (Mulvenon and Rattray, 2012). As cyberattacks can be easily routed through multiple networks or even proxies in a third country, it is very difficult to identify the intent of the strike and the responsible party. It is more difficult to deter by retaliation without identifying the real attacker. Offense is believed to have much more advantage over defense in cyberspace. The defender has to maintain a great wall for the entire system while the attacker only needs to find one single weak point. Offense dominance elicits a strong incentive to strike first. Additionally, cyber capabilities have become part of the "tool-box" to "manipulate the strategic environment" (Sheldon, 2012). As the entry barrier is extremely low and cyber weapons can be rapidly proliferated, it multiples the power of small and weak actors so that they can launch an asymmetric attack on major powers. Cyberspace has become "a perfect breeding ground for political disorder and strategic instability" (Kello, 2013b).

Furthermore, "the fundamental instability of cyberspace compounds the mistrust between China and the US" (Segal, 2013). All of the pessimistic discourse and growing concerns about the vulnerability of cyberspace are "motivated to no small extent by concerns about China's economic and military development" (Lindsay *et al.*, 2015a). Especially after the 2008 economic crisis, the relative decline of the US and the continuous rising of China make a collision between the established superpower and the emerging power very likely as the Thucydides trap forecasts. Henry

Kissinger warned that "enough material exists in China's quasi-official press and research institutes to lend some support to the theory that relations (between Washington and Beijing) are heading for confrontation rather than cooperation" (Kissinger, 2012). President Xi Jinping's promotion of the China Dream is perceived by Western scholars as a shift away from "hide and bide" to challenging the post-war order (Inkster, 2018). China's recent assertive foreign policy in both world affairs and periphery relations reflects its long-term strategic objective to replace the US as the superpower (Pillsbury, 2015). With China's increasingly hostile behavior in the East and South China Seas, the geopolitical competition makes a conflict scenario between Beijing and Washington very likely (Christensen, 2006; Copper, 2012; Glaser, 2017). Other flashpoints, including the Korean Peninsula and Taiwan Strait, can easily escalate to involve the US as well. This, in turn, leads to much more focus on how cyber capabilities can help the PLA compensate for the gap in physical military capabilities and gain leverage on the battlefield (Kraska, 2010; Lambeth, 2011; Reveron, 2012). A former US Air Force Chief of Information Operations predicted that during the conflict between the US and China over Taiwan, cyberwar would be essential (Barrett, 2005). China can not only attack infrastructure to undermine the will of the Taiwanese, but also interfere with the unclassified logistic systems to deter or delay US military intervention (Hannas *et al.*, 2013). It was also argued that China would leverage its unique advantage to recruit a huge population of patriotic hackers, netizens, or even technical school students as cyber militia and issue laptops to the populace to revive Chairman Mao's doctrine of the "people's war" (Blasko, 2001; Barrett, 2011; Klimburg, 2011; DeWeese, 2009; Mulvenon, 2009). "Let's say an emerging superpower would dedicate 20,000, 30,000, 40,000 people and then unleash that force at some point" (Skinner, 2008; Hjortdal, 2011), which would obviously be a disaster for the US. In a doomsday scenario, several thousand Americans would die, trains would derail, and satellites would fall; all of the critical infrastructure would be paralyzed (Clarke and Knake, 2014).

However, the extremity of this scenario is troubling for many reasons. The question of whether or not the nature of cyber technology leads to strategic instability deserves more careful examination in the first place. Analysts often overstate the animosity problem as a driving force of cyber warfare. It is true that the difficulty of attribution makes cyber espionage,

hacking, and other cyber disputes unresolvable. But, it is incorrect to apply the same logic to the analysis of cyber warfare as any war must have a strategic objective. "There is no sneaky way" to pass political intention to the adversary or subjugate the enemy (Betz and Stevens, 2011b). Serious cyber conflicts, like the 2008 Russo-Georgian or the Stuxnet, often develop under a greater geopolitical context, which provides important clues in identifying the attacker (Valeriano and Maness, 2015a). Without the protection of anonymity, the attacker has to think twice about retaliation or escalation before taking action. Although widely spread cyber technology and malware have largely lowered the barrier of entry for cyberattack, it does not mean that any state can launch a critical cyberattack against any infrastructure at any time as "the complexity of weaponization makes cyber offense less easy and defense more feasible than generally appreciated" (Lindsay, 2013c).

Additionally, cyber restraint exists between states as empirical study shows that despite the increasing frequency of cyber disputes (cyber espionage or other hacking activities), the severity level has remained very low and there is no evidence of any escalation in cyber conflicts (Valeriano and Maness, 2012a,b, 2014). For example, the US did not launch a direct cyberattack against Iraq, Afghanistan, or Libya despite the Stuxnet; Russia avoided using cyber weapons during the Crimea crisis after the 2008 Russo-Georgian conflict; China also used cyber capabilities minimally, only for CNE rather than destroying any infrastructure. There are many reasons why a state has to restrain the severity of its cyber operations and keep advanced cyber weapon secret. Most cyber weapons are one-time use as the zero-day exploits, once used, will no longer be the adversaries' weak points (Gartzke, 2013a; Rowe, 2008). To some extent, cyberattack is helping the rival discover system vulnerabilities, which means the more frequent the cyberattack, the stronger the defense it needs to challenge (Libicki, 2009). Additionally, malware can be reproduced and used to target the original attacker very quickly (Nye, 2011a; Farwell and Rohozinski, 2011). An extreme cyberattack may not only cause collateral damage to a third party and blowback to the initiators themselves, but also incur serious retaliation (Valeriano and Maness, 2015b). Last but not the least, the damage caused by cyberattack against a robust system with good resilience and backup is usually temporary, which means it can hardly change the fundamental balance of power between rivals. So what good would a major

cyberattack do if it faces so many uncertainties and brings so many negative consequences to the strategic calculation?

When analyzing the specific cyberwar scenario between China and the US, we should apply all of the counterarguments above. Despite the continuing revolution in military affairs (RMA), states must have a clear strategic goal behind its operations (Mansbach and Vasquez, 1981). Pessimists are used to exaggerate one side of the cyber capabilities and link the fear of new technology with a long-standing mistrust of China. However, basing policy and strategic advice on the "worst case scenario" analysis cannot improve this situation as misjudgment of states' intentions and the hostility of their words and actions will lead to overreaction and a downward spiral, which are the deep roots of security dilemma between states (Jervis, 1979, 1988). It is dangerous to make the "cyberwar threat from China' a normative view in the West" (Richards, 2014). In fact, many factors restrain states' cyber operations. No matter how used in tactical or strategic ways, a major cyberattack will bring negative consequences to the cost–benefit calculation. The attack may not be effective in the first place. It will also enhance the enemy's defense, cause collateral damage and blowback, and escalate into kinetic war. This is not to say that the PLA would not use its cyberwar capabilities even when reacting to a Taiwan contingency. However, it is not any single cutting-edge technology, but the balance of power and combination of strategies that will decide the outcome of large-scale military operations.

3. The Shift of China's Strategic Thinking on Cyberwar

Despite so many reasons for a self-restrained cyber behavior, most current English literature still argues that cyber warfare is appealing to China not only in regional conflicts, like the Taiwan Strait, but also in peacetime as it is in accordance with classical Chinese thinking on warfare, especially Sun Tzu's "subjugating the enemy's army without fighting" (Mazanec and Thayer, 2015b). There is no smoke without fire. In the early stages of the PLA's "informationization", Chinese strategists overemphasized cyber offense and the effectiveness of cyberattack as a coercive tool. But when Western scholars criticize China's "ideology of the offensive" as possibly leading to inadvertent escalation (Gompert and Libicki, 2014; see footnote 5),[5] most of

[5]For "ideology of the offensive" during the First World War, see Snyder (1989) and Van Evera (1999).

them fail to recognize that the PLA's interest in cyberwar capabilities has been "inspired in no small part by American writing and demonstrated ability in the field" (Lindsay *et al.*, 2015c; Inkster, 2016). Fortunately, many non-military analysts have joined the discussion after having studied their US counterparts' debate on cyber deterrence in recent years. More doubts and reflections have been made on offense dominance and cyber deterrence. However, as the US government continues its cyber deterrence strategy with a declaratory policy that reserves the right to retaliate cyberattack in any appropriate manner, China has been shifting to consideration of its own deterrence strategy as a reaction since 2015.

4. Offensive Dominance: 1990 to 2008

There are two historical trains of thought that illuminate China's understanding of cyberwar in the early stage. One stumbling block is that the "difference in terminology complicates the development of mutual understanding" between China and the US on strategic dialogue (Heginbotham *et al.*, 2017; Kulacki, 2011). For example, the Chinese term *weishe*, generally translated as "deterrence", encompasses both deterrence (preventing the target from taking an action) and compellence (forcing the target to take an action) (Guangqian and Youzhi, 2001; see footnote 6).[6] Especially during the Cold War, "Chinese strategists viewed "nuclear deterrence" as inherently aggressive Western behavior, akin to coercion or compellence, in which China did not see itself engaging. The origins of this thinking lie in the Chinese translation of the term "deterrence" (*weishe*), which is to use overwhelming military force (*wei*) to intimidate (*she*) an adversary into submission" (Bin, 2006; Fravel and Medeiros, 2010). The difference in glossary not only causes misunderstanding, but also reflects China's strategic thinking which is deeply rooted in its painful experience with the West since 1840. As "lagging behind leaves one vulnerable to attacks", Chairman Mao believed that the only way to break the nuclear monopoly of superpowers and avoid nuclear blackmail (coercion) was for China to have its own nuclear weapons. One prominent Chinese scholar summarized such strategic thinking as "anti-coercion" (Bin, 2006), which obviously influences the PLA's attitude toward its development of

[6]For the difference between deterrence and compellence, see Schelling (1966).

cyberwar capabilities. The second train of thought is that the PLA has not fought a war since 1979 while the US and its allies have demonstrated the growing role of advanced technology in modern warfare. Shocked by how easily the US defeated a Soviet-equipped Iraqi army during the First Gulf War, the PLA spared no effort to upgrade its information war capabilities in order to avoid falling behind and being humiliated again.

In the early stages of China's catching up with "informationization", the PLA emphasized cyber offense and preemptive strikes, and even characterized major cyberattack as a coercive tool against the US. The PLA strategists argued that as a "computer network war is an important means for paralyzing enemy" (Xiaoyan, 2002), "whoever possess superiority in integrated network electronic operations (a combination of cyber and electronic warfare) will then control the high point of future wars and will win future wars" (Shengwei, 2008). Cyberattack is perceived as low cost, covert, but extremely destructive, and the bar to enter is very low (Wenguang and Yuanlei, 2007; Shengwei, 2008; Liang *et al.*, 2009). Many writers who favor offense over defense even argue that "whoever strikes first prevails" (Yuliang, 2006a; Qingmin, 2002a; Linzhi, 1996). Through attacking the key nodes in either the enemy's C4ISR system or critical infrastructure, the PLA could acquire the upper hand in a battle against the stronger US military, create massive loss to its socio-economy, and eventually win the war (Yuliang, 2006b; Shengwei, 2008; Qingmin, 2002b).

However, the propensity to overemphasize the effectiveness of cyberattack exists not only in China, but also in the US as the debate on cyberwar has already demonstrated. And the military history has witnessed theorists repeating the same mistake of overemphasizing a single technology due to the "shock of the new'. For example, the "airpower has never lived up to the dreams of its most enthusiastic advocates" (Betz and Stevens, 2017) as the London Blitz turned out to be a failure. It is fortunate that many US scholars criticized these obsessions later, but it is unfortunate for China to have had such "ideology of the offensive" during the PLA's "informationization leap forward" till late 2000s.

5. Debate on Cyber Offense and Deterrence: 2009 to 2014

A widely held wrong impression is that Chinese strategists have a consensus on cyberwar and have not paid attention to the destabilizing

consequences brought by misunderstanding it (Lindsay *et al.*, 2015b). In fact, an increasing number of civilian researchers have joined the debate on cyberwar since 2008, and even some of the PLA strategists have voiced different opinions. Ventre's (2014) research on US discourse regarding China's cybersecurity issues reveals that 2008 was a "hinge point" when the Department of Defense began to express great concern over China's cyberattacks. In addition to the pressure from the US, continuous cyber incidents, such as the cyberattack against Estonia, Georgia, the Stuxnet against Iran, the Arab Spring, and the PRISM revealed by Edward Snowden, have had a profound impact on Chinese thinking on cybersecurity. The boom of cybersecurity issues attracted not only the PLA strategists, but also scholars and analysts from universities and think tanks to discuss its impact on national security, foreign policy, and economic development.

One of the important disagreements comes with the debate on cyber deterrence. In the early stage, the PLA strategists believed that the principles of mutually assured destruction could be applied to cyberspace (Academy of Military Science Strategic Studies Group, 2004–2005). As "hegemonic countries" like the US were developing cyber capabilities, China must also have its own cyber deterrent (Qingmin, 2002a). However, many non-military analysts began to doubt the effectiveness of cyber deterrence after studying American peers' comments on this topic. For example, professor He Qisong at Shanghai University of Political Science and Law published two papers in 2012 and 2013 in journals published by the China Institute of Contemporary International Relations and Peking University in which he summarizes the debate on cyber deterrence in the US (Qisong, 2012, 2013). Quoting James Lewis, David D. Clark, Richard A. Clarke, and Adam Segal, he notes that the attribution problem makes cyber deterrence very difficult. He further joins a discussion with Patrick Morgan, Herbert Lin, and Martin Libicki, and points out that a credible cyber deterrence must face challenges including how to demonstrate the power of cyber weapons and how to set the threshold neither too high nor too low. Associate researcher Ren Lin at China Academy of Social Science echoed this argument by saying that due to the problem of attribution, false flags, and the uncertainty of cyberattack, deterrence by retaliation is not practicable in cyberspace (Lin and Weian, 2015). Associate Professor Dong Qingling and Professor Dai Changzheng at the University of International Business and Economics published another paper in the top Chinese social

science journal (Qingling and Changzheng, 2012). They conducted a careful literature review on both sides of the cyber deterrence debate and concluded that a state's cyber strategy is determined by the risk preference of the leadership, a viewpoint very similar to Libicki's. Other commentators, such as Yu Xiaoqiu, a senior researcher at Central Compilation and Translation Bureau, a high-ranking think tank directed by the Chinese Communist Party, Ambassador Li Hong, the former secretary of China Arms Control and Disarmament Association, and Associate Professor Shen Yi from Fudan University wrote several articles in the People's Daily and People's Tribune in which they argue that the pursuit of cyber deterrence will increase the possibility of accidental wars and cause global instability (Xiaoqiu, 2011; Hong, 2011; Yi, 2011). Even PLA officers, such as colonel Liang Kui and Yang Yanbo, argue in the China National Defense Newspaper that as cyberattack usually causes no damage to physical assets or personnel casualties, and as the results of cyberattack are temporary and reversible, the credibility of cyber retaliation becomes very low (Kui, 2011; Yanbo, 2012). Although these discussions do not touch upon cyberwar directly, they help correct many key assumptions and misunderstandings widely held during the early stage. Since the effectiveness of cyberattack is largely uncertain, and usually limited (due to the enemy's superior defense) or even negative (due to collateral damage and blowback), it further weakens the advocation for cyber offense or coercion.

There are still PLA strategists who support cyber deterrence, but the argument is quite different compared to the "ideology of the offensive" seen in the first stage. Senior colonel Ye Zheng published an article, first in Chinese and later translated into English, on how to fight a cyberwar (Zheng and Baoxian, 2011; Lindsay *et al.*, 2015d). Ye states clearly that cyberwar capabilities are essential to national security and survival, and that weaker states can use cyber weapons against stronger rivals to win a fight (Lindsay *et al.*, 2015e). However, he also emphasizes that "cyberwarfare is also attractive for strong powers like the US, which can use it to supplement the exercise of military power or to expand the range of covert action options" (Lindsay *et al.*, 2015f). He further explains that "the US has established the world's first dedicated Cyber Command and fully functional cyberwarfare units in order to establish a controlling position over cyber power. Following this example, other countries are developing their own cyber power in competition" (Lindsay *et al.*, 2015g). The priority here

is therefore not to launch asymmetric attacks or coerce others, but to protect China itself from a potential destabilizing order. Beijing perceives severe threat from cyberspace, especially after Snowden's revelations about NSA operations. The US is considered not only to possess advanced cyber technology, but also to enjoy the advantage of human capital, training systems, and warfighting experience. As there are also many foreign industrial control systems used in China, it faces the high risk of a Stuxnet-like cyberattack (Shan, 2011; Qinzhi, 2013). A deteriorating cybersecurity situation provides good reasons for those who call for developing China's own cyber deterrence.

In the second stage, the so-called "ideology of the offensive" subsided, and there was no consensus as to what kind of strategy the PLA should take. The existing examples of cyberwar or serious cyber incidents led to the counterintuitive conclusion that cyber technology is used by great powers to bully the weak, not the opposite. Instead of advocating a preemptive strike, some PLA strategists argued that China must build up its own cyber deterrent against the increasing threat from the US. However, other analysts, especially from the non-military side, rebutted that the logic of deterrence could hardly be applied to cyberspace as the nature of the technology is so different from the past experience. Such counterargument was also largely based upon their peers' research in the US.

6. Back to Defense and Deterrence: Post-2015

However, as the practice of the US government and military was opposite to what the skeptics had expected, the debate on cyber deterrence in China also came to an end around 2015. Since cyber deterrence was confirmed once again as the key part of the US national cybersecurity strategy in the 2015 Department of Defense Cyber Strategy, both Chinese military and non-military strategists believe that it is time to develop their own cyber deterrence strategy. Since 2015, several important articles have been published in the journal published by the China Information Technology Security Evaluation Center, which is directed by the LSG for Cybersecurity and Informatization. One of Dong Qingling's articles argues that despite the many difficulties mentioned in the debate, cyber deterrence is still an important and necessary national security strategy (Qingling, 2016). He further points out that China has to understand the role of punishment in

different kinds of cyberattacks and clarify the responsibility of the third parties in order to promote such strategies. Of note, the journal indicates that Dong's research is a major project funded by the National Social Science Foundation (NSSF), which is closely tied to government policy-making. Professor Cheng Qun and He Qisong published another article that calls for cyber deterrence strategy with Chinese characteristics (Qun and Qisong, 2015). Qun and Qisong highlighted the idea of linking China's nuclear deterrence with cyber deterrence in order to prevent any major cyberattack from other big powers. They further explain that as a cyberattack against the C4ISR system is like shooting down an early warning satellite, it would very likely be followed by a nuclear strike. It may seem mad to retaliate against a cyberattack with a nuclear deterrent, but such irrational thinking is what makes the "balance of terror" successful. Coincidentally, the US Defense Science Board published a report several years ago that also proposes the same idea of connecting cyber and nuclear deterrence (The US Department of Defense and Defense Science Board, 2015). Qun and Qisong's argument also helps to correct the overemphasis on cyber strikes against an enemy's command and control system as it will cause the opponent to lose control of its forces and lead to a total war. Colonel Yuan Yi from the PLA Academy of Military Science also agrees with these arguments by analyzing how to establish China's cyber deterrence in details (Yi, 2015). She points out that it is essential to declassify the tests for some cyber weapons, demonstrate the PLA cyber equipment and broadcast the cyber drill in order to increase the credibility of cyber deterrence. She further notes that there is a balance between hiding and brandishing the cyber capabilities, which can perplex the enemy and dissuade potential attackers.

These points have been largely reflected in official documents recently published by the Chinese government and military. Although the China's Military Strategy in 2015 introduced how the PLA would protect cybersecurity without using the word deterrence, it tiptoed between cyber defense and deterrence strategy. "China will expedite the development of a cyber force, and enhance its capabilities of cyberspace situation awareness, cyber defense. . .so as to stem major cyber crises, ensure national network and information security, and maintain national security and social stability" (The State Council Information Office of the People's Republic of China, 2017). One year later, the Chinese National Cyberspace Security Strategy

criticized cyber deterrence for aggravating an arms race first. However, in the section on Strategic Tasks, it stated clearly that China would simultaneously develop "protection and deterrence", and "focus on identification, prevention, monitoring, early warning, response handling and other such segments" (Cyberspace Administration of China, 2016). Furthermore, it would "adopt all measures, including economic, administrative, scientific, technological, legal, diplomatic, and military measures" to protect its "information infrastructure and information resources" (Cyberspace Administration of China, 2016). Even the idea of cross-domain deterrence can be well inferred from these sentences. The latest Chinese International Strategy of Cooperation on Cyberspace follows the same pattern by criticizing the "deterrence buildup in cyberspace" in the beginning while proposing to "expedite the development of a cyber force and enhance capabilities. . .to prevent major cyber crisis" (Xinhua News, 2017). Although an official Chinese cyber deterrence strategy has yet to be established, reading between the lines reveals that this strategic thinking can be found in all of the current related documents.

The West may once again suspect China's true intentions when they see it opposing the idea of cyber deterrence in rhetoric while nonetheless developing its own capabilities to establish credible cyber deterrent. The reason for saying one thing and doing another here is again related to China's strategic culture. As discussed in the beginning of Sec. 4, deterrence is a negative word in Chinese. Beijing has long perceived deterrence as an offensive or coercive strategy used by the "hegemonic states". In this context, developing a deterrence strategy seems contradictory to the principle of peace consistently advocated by the Chinese government. What China therefore strongly opposes is coercion, not deterrence. Deterrence can promote a purely defensive posture, which is precisely what China says about its nuclear deterrence. It nonetheless took several decades for Beijing to finally accept the word "deterrence" as its nuclear strategy.

7. Conclusion

Most current English literature criticizes China's accumulation of cyberwar capabilities and predicts a very likely cyberwar launched by the PLA against the US. However, they ignore many constraining factors faced by the PLA, such as the uncertain effectiveness of a large-scale cyberattack,

which may be useless when faced with an adversary's robust system. It would also bring serious negative consequences, such as collateral damage to the third party or blowback. Without the cover of anonymity, it would definitely incur retaliation or even escalation into total war. So the PLA has to be very cautious about initiating any major cyberattack.

This paper does not deny the fact that many Chinese military strategists advocate cyber weapons in an asymmetric attack against the US military and civilian targets. However, the overemphasis on the effectiveness of cyberattack and "ideology of the offensive" were early immature thinking due to the shock of the Gulf War and the pressure of falling behind again during the new round of RMA. In fact, China's strategic thinking on cyberwar started to shift around 2008 with a serious debate on cyber offense and deterrence. On the one hand, many non-military scholars drew upon the latest research from their peers abroad to criticize cyber deterrence strategy. The uncertainties of cyberattack not only weaken the credibility of retaliation, but also its effectiveness as a coercive tool. On the other hand, some PLA strategists maintained that it was necessary to establish a powerful cyber force in order to deter cyberattack from the US. The "ideology of the offensive" in the early stage rarely appeared. The debate ended around 2015 with an increasing number of analysts calling for China's own cyber deterrence strategy as a reaction to the continuous development of cyber deterrence by the US. The latest Chinese official documents on cybersecurity have largely reflected the shift in strategic thinking.

The US perceptions and practice of cyberwar are the main drivers of China's shift in strategy thinking. Both Chinese military and non-military strategists play an intermediary role in passing these ideas and shaping the policy. In the early stage, PLA experts not only learned cyber technology as a new RMA from the US, but also exaggerated the effectiveness of cyberattack as many theorists did. Later, with civilian scholars following the research of their peers in the US, they began to question the effectiveness of cyberattack. Finally, Beijing may soon imitate Washington's cyber deterrence strategy as a reactive policy. It is no coincidence that even the names of China's recent cyber strategy documents are the same as those of the US. Both military and non-military strategists play an essential role in the evolution of China's strategic thinking on cyberwar. In order to preserve the stability between China and the US in cyberspace, the dialogue between intellectuals from both sides will be very helpful to clarify key concepts,

initiate policy debate, reflect on misleading principles, and even change the input of policy-making.

References

Academy of Military Science Strategic Studies Group (2004–2005), *Strategic Deterrence* [Lun Zhanlue Weishe] (Beijing: China Military Science), p. 238.

Adam Segal (2013), "The Code Not Taken: China, the United States, and the Future of Cyber Espionage," *Bulletin of the Atomic Scientists*, 69(5): 38–45.

Alexander Klimburg (2011), "Mobilising Cyber Power," *Survival*, 53(1): 41–60.

Alice L. Miller (2014), "More Already on the Central Committee's Leading Small Groups," *China Leadership Monitor*, 44: 1–8.

Barrington M. Barrett (2005), "Information Warfare: China's Response to U.S. Technological Advantages," *International Journal of Intelligence and CounterIntelligence*, 18(4): 682–706.

Benjamin Lambeth (2011), "Airpower, Spacepower and Cyberpower," *Joint Force Quarterly*, 60: 47–53.

Bin Li (2006), "Analysis of China's Nuclear Strategy," [Zhongguo Hezhanlue Bianxi], *Shijiejingji yu zhengzhi*, 9: 16–22.

Bin Li (2008), "Analysis of China's Nuclear Strategy," pp. 16–22.

Bonnie S. Glaser (2017), "Armed Clash in the South China Sea," Contingency Planning Memorandum No. 14, Council on Foreign Relations, http://www.cfr.org/asia-and-pacific/armed-clash-south-china-sea/p27883. Accessed on June 15, 2017.

Bonnie S. Glaser and Phillip C. Saunders (2002), "Chinese Civilian Foreign Policy Research Institutes: Evolving Roles and Increasing Influence," *The China Quarterly*, 171: 597–616.

Brandon Valeriano and Ryan C. Maness (2012a), "Persistent Enemies and Cybersecurity: The Future of Rivalry in an Age of Information Warfare," in Derek S. Reveron, eds., *Cyber Challenges and National Security*, (Washington, DC: Georgetown University Press), pp. 139–158.

Brandon Valeriano and Ryan Maness (2012b), "The Fog of Cyberwar: Why the Threat Doesn't Live up to the Hype," *Foreign Affairs*, November 21, 2012, https://www.foreign-affairs.com/articles/2012-11-21/fog-cyberwar. Accessed on June 15, 2017.

Brandon Valeriano and Ryan C. Maness (2014), "The Dynamics of Cyber Conflict Between Rival Antagonists, 2001–2011," *Journal of Peace Research*, 51(3): 347–360.

Brandon Valeriano and Ryan C. Maness (2015a), *Cyber War Versus Cyber Realities: Cyber Conflict in the International System* (Oxford: Oxford University Press), p. 10.

Brandon Valeriano and Ryan C. Maness (2015b), *Cyber War Versus Cyber Realities: Cyber Conflict in the International System* (USA: Oxford University Press).

Brian M. Mazanec and Bradley A. Thayer (2015a), *Deterring Cyber Warfare: Bolstering Strategic Stability in Cyberspace* (New York: Palgrave Macmillan), p. 12.

Brian M. Mazanec and Bradley A. Thayer (2015b), *Deterring Cyber Warfare: Bolstering Strategic Stability in Cyberspace* (New York: Palgrave Macmillan), p. 32.

Cyberspace Administration of China (2016), translated by China Copyright and Media, Cyberspace Administration of China, https://chinacopyrightandmedia.wordpress.com/2016/12/27/national-cyberspace-security-strategy/. Accessed on June 15, 2017.

David J. Betz and Tim Stevens (2017), *Cyberspace and the State: Toward a Strategy for Cyber-Power*, (Abingdon: Routledge), p. 88.

Daniel Ventre (ed.) (2014), *Chinese Cybersecurity and Defense* (New Jersey: ISTE Ltd. and John Wiley & Sons Inc.), pp. 278–282.

David C. Gompert and Martin C. Libicki (2014), "Cyber Warfare and Sino-American Crisis Instability," *Survival*, 56(4): 7–22.

David J. Betz and Tim Stevens (2011b), *Cyberspace and the State: Toward a Strategy for Cyber-Power*, (Abingdon: Routledge), p. 95.

David Shambaugh (2002), "China's International Relations Think Tanks: Evolving Structure and Process," *The China Quarterly*, 171: 581.

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

Dennis Blasko (2001), "PLA Force Structure: A 20-Year Retrospective," in James C. Mulvenon and Andrew N. D. Yang, eds., *Seeking Truth from Facts: A Retrospective on Chinese Military Studies in the Post-Mao Era* (Sanata Monica, CA: RAND), pp. 51–86.

Derek Reveron (ed.) (2012), "An Introduction to National Security and Cyberspace," in *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World* (Washington, DC: Georgetown University Press), pp. 3–20.

Erik Gartzke (2013a), "The Myth of Cyberwar: Bringing War on the Internet Back Down to Earth," *International Security*, 38(2): 41–73.

Eric Heginbotham *et al.* (2017), "China's Evolving Nuclear Deterrent: Major Drivers and Issues for the United States," RAND Corporation, http://www.rand.org/content/dam/rand/pubs/research_reports/RR1600/RR1628/RAND_RR1628.pdf. Accessed on June 15, 2017.

Gregory Kulacki (2011), "Chickens Talking With Ducks: The U.S.-Chinese Nuclear Dialogue," October 2011, https://www.armscontrol.org/act/2011_10/U.S._Chinese_Nuclear_Dialogue. Accessed on June 15, 2017.

Guangqian Peng and Youzhi Yao (2001), *The Science of Strategy* [Zhanluexue] (Beijing: Military Sciences Press), p. 232.

Henry A. Kissinger (2012), "The Future of US-Chinese Relations," *Foreign Affairs*, 91(2): 44–45.

Hong Li (2011), "The Jungle Law Will Increase the Risks of Cyberwar," [Conglin Faze Jiaju Wangluo Zhanzheng Fengxian], *People's Tribune*, 16: 22–23.

Jack L. Snyder (1989), *The Ideology of the Offensive: Military Decision Making and the Disasters of 1914* (New York: Cornell University Press).

James P. Farwell and Rafal Rohozinski (2011), "Stuxnet and the Future of Cyber War," *Survival*, 53(1): 23–40.

James Mulvenon (2009), "PLA Computer Network Operations: Scenarios, Doctrine, Organizations, and Capability," in Roy Kamphausen, David Lai and Andrew Scobell, eds., *Beyond the Strait: PLA Missions Other Than Taiwan*, (Washington, DC: National Bureau of Research), pp. 277–278.

James Kraska (2010), "How the US Lost the Naval War of 2015," *Orbis*, 54(1): 35–45.

James C. Mulvenon and Gregory J. Rattray, (eds.) (2012), *Addressing Cyber Instability* (Washington, DC: Cyber Conflict Studies Association).

James G. McGann (2017), *2016 Global Go to Think Tank Index Report*, Think Tanks and Civil Societies Program (TTCSP), http://repository.upenn.edu/cgi/viewcontent.cgi?article=1011&context=think_tanks. Accessed on June 15, 2017.

John Arquilla and David Ronfeldt (1993), "Cyberwar is Coming!" *Comparative Strategy*, 12(2): 141–165.

John F. Copper (2012), "Island Grabbing in the East China Sea," *The National Interest*, September 14, 2012.

John Sheldon (2012), "Toward a Theory of Cyber Power: Strategic Purpose in Peace and War," in Derek Reveron, ed., *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, (Washington, DC: Georgetown University Press), pp. 208–209.

Jon Lindsay (2013a), "Stuxnet and the Limits of Cyber Warfare," *Security Studies*, 22(3): 372.

Jon Lindsay (2013b), "Stuxnet and the Limits of Cyber Warfare," 22(3): 365–404.

Jon Lindsay (2013c), "Stuxnet and the Limits of Cyber Warfare," *Security Studies*, 22(3): 365–404.

Jon R. Lindsay, Tai Ming Cheung and Derek S. Reveron (2015a), *China and Cybersecurity* (Oxford: Oxford University Press), p. 2.

Jon R. Lindsay, Tai Ming Cheung and Derek S. Reveron (2015b), *China and Cybersecurity* (USA: Oxford University Press), p. 18.

Jon R. Lindsay, Tai Ming Cheung and Derek S. Reveron (2015c), *China and Cybersecurity* (Oxford: Oxford University Press), pp. 344–345.

Jon R. Lindsay, Tai Ming Cheung and Derek S. Reveron (2015d), *China and Cybersecurity* (Oxford: Oxford University Press), p. 125.

Jon R. Lindsay, Tai Ming Cheung and Derek S. Reveron (2015e), *China and Cybersecurity* (Oxford: Oxford University Press), p. 344.

Jon R. Lindsay, Tai Ming Cheung and Derek S. Reveron (2015f), *China and Cybersecurity* (Oxford: Oxford University Press), p. 124.

Jon R. Lindsay, Tai Ming Cheung and Derek S. Reveron (2015g), *China and Cybersecurity* (Oxford: Oxford University Press), pp. 124–137.

Joseph S. Nye (2011a), "Nuclear Lessons for Cyber Security?" *Strategic Studies Quarterly*, 5(4): 20–21.

Joseph S. Nye (2011a), "Nuclear Lessons for Cyber Security?" pp. 18–38.

Julian Richards (2014), *Cyber-war: The Anatomy of the Global Security Threat* (New York: Palgrave Macmillan), p. 54.

Kui Liang (2011), "Cyber Deterrence: Ineffective Despite Powerful," [Wangluo Weishe: Weier Nanshe], *Zhongguo Guofangbao*, August 8.

Li Cheng (2009), "China's New Think Tanks: Where Officials, Entrepreneurs, and Scholars Interact," *China Leadership Monitor*, 29, pp. 1–21, http://media.hoover.org/sites/default/files/documents/CLM29CL.pdf. Accessed on June 15, 2017.

Liang Shang, Guoxin Yang, Jianlai Shi and Shilong Sui (2009), "Network Warfare Troops: The New Favorite of Armies in Various Countries," [Wangluozhan Budui – Geguo Junzhong Xinchong], *Guofang Keji*, 30(4): 89.

Lin Ren and Weian Gong (2015), "The Strategic Choice of Cyber Security," [Wangluo Anquande Zhanlue Xuanze], *Shijie Jingjiyu Zhengzhi*, 5: 40–58.

Linzhi Lu (1996), "Preemptive Strikes are Crucial in Limited High-tech Wars," *Jiefangjun Bao*, February 7.

Lucas Kello (2013a), "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft," *International Security*, 38(2): 21.

Lucas Kello (2013b), "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft," *International Security*, 38(2): 7–40.

Magnus Hjortdal (2011), "China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence," *Journal of Strategic Security*, 4(2): 8.

Martin C. Libicki (2009), *Cyberdeterrence and Cyberwar* (Santa Monica: RAND Corporation), pp. xiv–xv.

Martin C. Libicki (2009), *Cyberdeterrence and Cyberwar* (Santa Monica: RAND Corporation), pp. xiv–xv.

Mike McConnell (2010), "How to Win the Cyber-War We're Losing," *Washington Post*, February 28, 2010.

Miriam Dunn-Cavelty (2008), *Cyber-security and Threat Politics: US Efforts to Secure the Information Age* (New York: Routledge), p. 1.

Michael Pillsbury (2015), *The Hundred-Year Marathon: China's Secret Strategy to Replace America as the Global Superpower* (New York: Henry Holt and Company).

National Research Council of the National Academies (2012), *Terrorism and the Electric Power Delivery System* (Washington, DC. National Academies Press), p. 16.

Nigel Inkster (2016), *China's Cyber Power* (New York: Routledge).

Nigel Inkster, *China's Cyber Power*, p. 98.

Nigel Inkster (2016), *China's Cyber Power* (New York: Routledge), p. 12.

Peter W. Singer and Allan Friedman (2014), *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford: Oxford University Press), p. 7.

Qun Cheng and Qisong He (2015), "To Establish China's Cyber Deterrence Strategy," [Goujian Zhongguo Wangluo Weishe Zhanlue], *Zhongguo Xinxi Anquan*, pp. 40–42.

Qingmin Dai, *Integrated Network Electronic Warfare* [Wangdian Yitizhan], pp. 107–108, pp. 113–114, p. 160.

Qingmin Dai (2002a), *Integrated Network Electronic Warfare* [Wangdian Yitizhan] (Beijing: Liberation Army Press).

Qingmin Dai (2002b), *Integrated Network Electronic Warfare* [Wangdian Yitizhan] (Beijing, China: PLA Press), p. 32.

Qingling Dong and Changzheng Dai (2012), "Cyber Deterrence: Is Retaliatory Strategy Possible?" [Wangluo Kongjian Weishe: Baofu Shifou Kexing], *Shijie Jingjiyu Zhengzhi*, 7: 99–116.

Qingling Dong (2016), "Cyber Deterrence and Its Key Questions," [Wangluo Kongjian Weishe Yanjiu Jiqi Quanjian Wenti], *Xinxi Anquan Yanjiu*, pp. 920–925.

Qinzhi Wei (2013), "Industrial Control System Security Situation and Safety Strategy Analysis," [Gongye Kongzhi Xitong Anquan Xianzhuangyu Anquan Celue Fenxi], *Xinxi Anquanyu Jishu*, 2: 23–24.

Qisong He (2013), "Debating Deterrence in the Cyber Space in the US," [Meiguo Wangluo Weishe Lilun Zhizheng], *Guoji zhengzhi yanjiu*, 34(2): 53–74.

Qisong He (2012), "Summary of the US Research on Cyber Deterrence in Recent Years," [Jinnian Meiguo Wangluo Weishe Lilun Yanjiu Shuping], *Xiandai Guoji Guanxi*, 10: 7–10.

Richard Clarke and Robert Knake (2010), *Cyber War: The Next Threat to National Security and What to Do About It* (New York: Harper Collins), p. 32.

Richard W. Mansbach and John A. Vasquez (1981), *Search of Theory: A New Paradigm for Global Politics* (New York: Columbia University Press).

Richard Clarke and Robert Knake (2014), *Cyber War: The Next Threat to National Security and What to Do About It* (New York: Harper Collins), p. 67.

Robert Jervis (1979), "Deterrence Theory Revisited," *World Politics*, 31(2): 289–324.

Robert Jervis (1988), "War and Misperception," *The Journal of Interdisciplinary History*, 18(4): 685.

Roderick Macfarquhar (ed.) (2011), *The Politics of China: Sixty Years of the People's Republic of China*, 3rd Edn. (Cambridge: Cambridge University Press), Chap. 5.

Rowe (2008), "Ethics of Cyber War attacks', in Lech J. Janczewski and Andrew M. Colarik, eds. *Cyber Warfare and Cyber Terrorism*, (PA: Information Science Reference), pp. 105–111.

Shan Li (2011), "Lifting the Veil of the Stuxnet Mystery," [Xiankai Stuxnet Bingdu Shenmide Miansha], *Kexueyu Wenhua*, 4: 25.

Shengwei Guo, *Informationized War and Network Electronic Units*, pp. 257–259, pp. 265–266, pp. 275, p. 364.

Shengwei Guo, *Informationized War and Network Electronic Units* [Xinxihua Zhanzhengyu Wangdian Budui], p. 223, p. 280, p. 281.

Shengwei Guo (2008), *Informationized War and Network Electronic Units*[Xinxihua Zhanzhengyu Wangdian Budui] (Beijing: National Defense University Press), p. 1.

Steve DeWeese (2009), "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation," *Northrop Grumman*, October 9, p. 7.

Stephen W. Van Evera (1999), *Causes of War: Power and the Roots of Conflict* (New York: Cornell University Press).

The Economist (2017), "Cyberwar," http://www.economist.com/node/16481504. Accessed on June 15, 2017.

The State Council Information Office of the People's Republic of China (2017), "China's Military Strategy," https://news.usni.org/2015/05/26/document-chinas-military-strategy. Accessed on June 15, 2017.

The US Department of Defense and Defense Science Board (2015), *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat* (USA: CreateSpace Independent Publishing Platform).

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

Thomas J. Christensen (2006), "Fostering Stability or Cheating a Monster? The Rise of China and US Policy Toward East Asia," *International Security*, 31(1): 81–126.

Thomas C. Schelling (1966), *Arms and Influence* (New Haven: Yale University Press), pp. 69–78.

Tony Skinner (2008), "War and PC: Cyberwarfare," *Jane's Defence Weekly*, September 19.

M. Taylor Fravel and Evan S. Medeiros (2010), "China's Search for Assured Retaliation: The Evolution of Chinese Nuclear Strategy and Force Structure," *International Security*, 35(2): 71.

US Department of Defense (2011), *Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms*, p. 93.

U.S.–China Economic and Security Review Commission (2017), *2007 Report to Congress*, https://www.uscc.gov/sites/default/files/annual_reports/2007-Report-to-Congress.pdf. Accessed on June 15, 2017; "Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage," http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-066.pdf. Accessed on June 15, 2017.

William C. Hannas, James Mulvenon and Anna B. Puglisi (2013), *Chinese Industrial Espionage: Technology Acquisition and Military Modernization* (New York: Routledge), p. 221.

Wenguang Xiao and Yuanlei Li (2007), "Computer Networks in Future Wars," [Jisuanji Wangluoyu Weilai Zhanzheng], *Jiangsu Hangkong*, 1: 31.

Xiaoyan Xu, (ed.) (2002), *The Science of Information Operations*[Xinxi Zuozhanxue] (Beijing: Liberation Army Press), p. 167.

Xiaoqiu Yu (2011), "Cyber Deterrence is a Dangerous Game," [Wangluo Weisheli Shige Weixiande Youxi], *People's Daily*, July 25.

Xinhua News (2017), "International Strategy of Cooperation on Cyberspace," http://news.xinhuanet.com/english/china/2017-03/01/c_136094371.htm. Accessed on June 15, 2017.

Xufeng Zhu (2011a), "Government Advisors or Public Advocates? Roles of Think Tanks in China from the Perspective of Regional Variations," *The China Quarterly*, 207: 672.

Xufeng Zhu (2011b), "Government Advisors or Public Advocates? Roles of Think Tanks in China from the Perspective of Regional Variations," *The China Quarterly*, 207: 678.

Yanbo Yang (2012), "Pay Attention to the US Cyber Deterrence Strategy," [Jujiao Meijun "Wangluo Weishe" Zhanlue], *Zhongguo Guofangbao*, January 9.

Yi Shen (2011), "The Pandora Box of the US Cyber Strategy is Disturbing the World," [Meiguo Wangluo Zhanlue "Mohe" Jiaoluan Shijie], *People's Tribune*, 16: 25–26.

Yi Yuan (2015), "Analysis on the Characteristics of Cyber Deterrence and the Key to Application," [Qianxi Wangluo Kongjian Weishede Tezheng Leixinghe Yunyong Yaodian], *Zhongguo Xinxi Anquan*, pp. 43–46.

Yuliang Zhang, (ed.) (2006a), *The Science of Campaigns* [Zhanyixue] (Beijing: National Defense University Press), p. 163;

Yuliang Zhang, (ed.) (2006b), *The Science of Campaigns* [Zhanyixue] (Beijing: National Defense University Press), p. 90.

Zheng Ye and Baoxian Zhao (2011), "How to Fight a Cyberwar?" [Wangluozhan, Zenmezhan], *Zhongguo Qingnianbao*, June 3.