Institution Building and Cyberwarfare Capabilities in China: A Study of Doctrine and Civil Military Relations

By Attila Arslaner, and Petro Voyatzakis
Concordia University
Montreal, Canada

Introduction

As Saddam Hussein's army was handed a swift and decisive defeat at the conclusion of Operation Desert Storm in 1991, the political and military leaders in China were watching intently. They were shocked at the logistical feat of waging a war halfway across the world with a seemingly short time to prepare. [1] Thus, began a series of reforms leading to the current state of the Chinese military. The prior assumption for the Chinese had been that they could wage a conventional war along the lines of their experience in the Sino-Vietnamese war. Since observing the 1991 Iraq war and the 1996 operations against Yugoslavia, they realized how far back they had fallen. The publication of the book "Unrestricted Warfare" in 1999 by two Chinese colonels, outlining the fundamental changes to come in fighting wars, reflected this sentiment perfectly.[2] Though by no means an official publication, it was an indication of the beginning of the shift in perceptions in China.

Given this, we will be examining the evolution of Chinese doctrine in one domain, in how it has developed its Computer Network Operations (CNO) capabilities. This paper aims to situate these developments it in the context of the recent modernization of the Chinese People's Liberation Army (PLA), with the aim of predicting potential behavior in case of an increase in

[1] Dean Cheng, "Chinese Lessons from the Gulf Wars," in *Chinese Lessons from Other Peoples ' Wars*, ed. Andrew Scobell and Roy Kamphausen (Carlisle, PA: Army War College Press, 2011), 153–200.
[2] Qiao Liang and Wang Xiangsui, *Unrestricted Warfare* (Beijing: PLA Literature and Arts Publishing House, 1999).

tensions with China. We argue given that the PLA is still in the process of modernization, it is currently reliant on a transient doctrine. Save for an extreme contingency, they would most likely not actively seek conflict. At present, if tensions were to rise, it would likely result in the utilization of techniques low in relative sophistication, nevertheless high in effectiveness. This paper will be taking into account the institutional barriers in China, in order to comprehend how the problem is perceived within their given institutional framework. Additionally, we will be looking to the behavior of other countries and attempt to set a precedence for how China might behave in cyberspace.

We will first examine the current state of Chinese and North Korean institutions, followed by a short study of the difficulties surrounding deterrence and escalation control in the cyber domain. Lastly, we will examine the exploitation of computer network operations as an extension of their respective countries' foreign policies using a case study of North Korean and Russian use of cyberattacks.

Institutional and Doctrinal Study

To understand our adversaries' capabilities and the challenge they pose to the status quo, it is vital to analyze the institutions they have in place and the inherent limits these institutions present. The nature of civil-military relations in China are fundamentally different than in the west. Mao Zedong's dictum "Political power grows out of the barrel of a gun" [3] has shaped the role of the PLA in its political capacity as the army of the Chinese Communist Party (CCP). This can be explained by how the composition of the CCP has changed over time; with the retirement of the veterans of the civil war, a generation of leaders with no military experience have taken

[3] Mao Zedong, *Problems of War and Strategy* (Beijing: Foreign Language Press, 1960). 13

over. Through this time, it has moved toward an institutional divide fragmented by principal agent problems and fractured in its military decision-making structures. The founding generation of the Chinese leadership were both political and military leaders. They held dual roles and had a more personalistic relationship with the military.[4] Having fought together during multiple wars made for this close cooperation.[5] Since that time, the only point of political control over the military has been and continues to be the leader of China, who typically is also the chairman of the Central Military Commission (CMC), the highest decision-making body for the PLA.[6] Thus, as the tenures of Jiang Zemin (1989-2002) and Hu Jintao (2002-2012) as General Secretary began, they faced multiple issues regarding control over the military. These leaders, both of whom held no military experience, signaled a shift from the prior generation of leaders, and for a diverging civil-military relationship in China.

A particular example of the loss of control, Xu Caihou and Guo Boxiong, two highly influential leaders in the PLA under Hu Jintao, were involved in multiple corruption scandals including the sale of military ranks.[7] In response to the scandals, official PLA publications put forward the standard propagandistic line, that the PLA should continue to "uphold the party's absolute leadership over the army" to prevent corruption in the future.[8] This can be categorized as a principal agent problem, defined by a clear disconnect between the top leadership and the

[4] James C. Mulvenon, *Professionalization of the Senior Chinese Officer Corps: Trends and Implications* (Santa Monica, CA: RAND Corp., 1997). 25
[5] Mulvenon. 57
[6] Andrew Scobell, Phillip Saunders, and Seth Jones, *PLA Influence on China's National Security Policymaking* (Stanford, CA: Stanford University Press, 2015), https://doi.org/10.7249/cb550. 74
[7] Chien Wen Kou, "Xi Jinping in Command: Solving the Principal-Agent Problem in CCP-PLA Relations?," *The China Quarterly* 232 (2017), https://doi.org/10.1017/S0305741017001321. 868
[8] "Guo Boxiong and Xu Caihou's Corruption Problem Is Not the Crux of Their Problem [郭伯雄、徐才厚贪腐问题不是他们问题的要害]," QQ News, 2016, https://news.qq.com/a/20160527/018042.htm?utm_source=The+Sinocism+China+Newsletter&utm_campaign=472b96a287-Sinocism05_30_165_30_2016.

military. In the case of Hu Jintao, it quickly became apparent that he did not have the experience to adequately oversee the military, this left a rudderless military to its own devices, forming a host of diverging interests and creating a principal agent problem.[9] With such a fragmented structure in place, the emergence of corruption scandals is expected. To further illustrate these diverging interests, the first test flight of the J-20 fighter coincided with the visit to China of US Defense Secretary Robert Gates in 2011.[10] Hu Jintao feigned ignorance at the occurrence of the test flight, which is plausible given his more distanced approach in dealing with the military.[11] This evidently illustrates a problem in how they are to project their capabilities to other countries.

The cybernetic model of decision making puts forth that when complex systems exclude an important component of their process, it leads to dysfunctions.[12] For instance, in international relations, if a military were to take action without diplomatic support from its foreign ministry, or vice versa, it would lead to a misaligned response.[13] For our consideration of China, as there emerged the separation among civil and military elites and their decision making, it is conceivable that there would be friction in any potential military response by China.

As president, Xi Jinping has taken a great interest in the PLA and has attempted to mend this discord through a series of comprehensive reforms. Through this he has concentrated more

[9] Kou, "Xi Jinping in Command: Solving the Principal-Agent Problem in CCP-PLA Relations?"
[10] Elisabeth Bumiller and Michael Wines, "China Tests Stealth Fighter as Gates Visits," The New York Times, 2011, https://www.nytimes.com/2011/01/12/world/asia/12fighter.html.
[11] Scobell, Saunders, and Jones, *PLA Influence on China's National Security Policymaking*.
[12] John Steinbruner, *The Cybernetic Theory of Decision* (Princeton, NJ: Princeton University Press, 1974).
[13] Julian Schofield, *Militarization and War* (New York, NY: Palgrave Macmillan, 2007). 14

control in himself by removing alternate sources of influence within the PLA,[14] and seeking to establish an improved institutional foundation of civilian oversight in the military for the future.[15] One of the long-term objectives from the turn of the century has been to establish an army capable of joint operations. This has been a central point of Xi Jinping's reforms, yet how this will be achieved remains unclear.[16] Furthermore, the system remains very much flawed as Xi himself, with limited military experience, still relies on the military for advice about itself.[17] A Chinese defense white paper from 2019 takes a step towards recognizes these shortcomings and states that they are falling short of their 2020 goals toward modernization as it remains "in urgent need of improving its informationization".[18] This could be explained by an institutional resistance to change, even as Xi Jinping has faced little overt resistance through this period; the PLA is normally slow to embrace any changes.[19]

Views of Computer Network Exploitation in China

This consideration of civil-military relations and of the structure of the PLA are highly relevant in looking at how the use of network electronic warfare is perceived in China. Cyberspace as a domain is particularly prominent in the Chinese literature on escalation.[20] Escalation as a whole is perceived to be predictable, controllable, and in following certain set

[14] Timothy R. Heath, "The Consolidation of Political Power in China Under Xi Jinping: Implications for the PLA and Domestic Security Forces" (RAND Corp., n.d.), https://www.rand.org/pubs/testimonies/CT503.html.
[15] Kou, "Xi Jinping in Command: Solving the Principal-Agent Problem in CCP-PLA Relations?" 872
[16] Cortez A. III Cooper, *PLA Military Modernization: Drivers, Force Restructuring, and Implications* (Santa Monica, CA: RAND Corp., 2018), https://doi.org/10.7249/ct488.
[17] Kou, "Xi Jinping in Command: Solving the Principal-Agent Problem in CCP-PLA Relations?"
[18] The State Council Information Office of the People's Republic of China, *China's National Defense in the New Era.* (Beijing: Foreign Language Press, 2019).
[19] Phillip Saunders et al., eds., *Chairman Xi Remakes the PLA: Assessing Chinese Military Reforms* (Washington, DC: National Defense University Press, 2019). 110
[20] Burgess Laird, "War Control: Chinese Writings on the Control of Escalation in Crisis and Conflict" (Washington, DC, 2017).

rules.[21] Information technology presents a new front of vulnerabilities, but also in further pushing this idea of predictability forward. The literature in China sees that information technology makes it such that no action taken by any side toward escalation would come as a surprise.[22] China assumes that as technology improves and achieves greater interconnectivity, the military will be ever closer to perfect information. Subsequently, it presents a range of "soft targets," i.e., not leading to the loss of life, which would supposedly allow for a more finely tuned escalatory or de-escalatory signaling in the event of a crisis.[23]

This leads to the idea expressed by multiple publications in China which sees information warfare as a war of systems.[24] In order to be able to effectively attack an adversary's C4ISR infrastructure and seek information superiority, an army capable of operating in complex environments stands as a crucial prerequisite.[25] Since, as outlined above, the PLA is currently incapable of joint operations across services, as it is not supported by a robust infrastructure for sharing information, their present doctrine must accommodate for this. In case of war today, they attempt to project a certain level of readiness even with a lower level of modernization,[26] all the while continuing work in standardizing capabilities across services.[27] An example of the lack of progress in this regard can be seen with a wargame conducted in 2018; an elite brigade equipped

[21] Alison A. Kaufman and Daniel M. Harnett, "Managing Conflict: Examining Recent PLA Writings on Escalation Control" (Arlington, VA, 2016).
[22] Laird, "War Control: Chinese Writings on the Control of Escalation in Crisis and Conflict." 15
[23] Laird. 15
[24] Zifeng Dong [**董子峰**], *The Transformation of Combat Effectiveness [战斗力生成模式转变]* (Beijing: 军事科学出版社, 2012).
[25] Ilan Berman, *The Logic of Irregular War* (Lanham: Rowmand & Littlefield, 2017). 13
[26] Kevin McCauley, "System of Systems Operational Capability: Key Supporting Concepts for Future Joint Operations," The Jamestown Foundation, 2012, https://jamestown.org/program/system-of-systems-operational-capability-key-supporting-concepts-for-future-joint-operations/.
[27] The State Council Information Office of the People's Republic of China, *China's National Defense in the New Era.*

with the latest Type 99A tank lost to a brigade with older equipment.[28] This indicates a lack of familiarity with and diffusion of the most modern technology even among the most elite soldiers. Furthermore, the perceptions of escalation control as outlined in the Chinese literature seems unfeasible given the lack of civilian oversight in the military's overall performance, raising doubts as to the ability to coordinate a coherent message and projection of capabilities. These inefficiencies are points increasingly voiced in the PLA's own publications,[29] reflecting Hu Jintao's[30] and Xi Jinping's[31] expression of the consistent problems they perceived in the PLA. Though in these articles and a significant portion of the literature, a true awareness of the root causes is somewhat lacking. Where the system is inherently at fault, the Chinese are unwilling to challenge the status quo. This is evident in the tone of much of the literature pushing for a further centralization and encouraging an adherence to the policies and actions of the leadership; mirroring the party line.[32] Chinese evaluations see this it as a lack of technology,[33] rather than a faulty institutional culture, appearing seemingly more concerned with keeping control of the PLA, rather than creating the necessary conditions for innovation.

---

[28] Xuanzun Liu, "PLA Moves to Integrate Techniques, Tactics with New Weapons Systems - Global Times," Global Times, 2019, http://www.globaltimes.cn/content/1136390.shtml.

[29] Dennis J. Blasko, "The Chinese Military Speaks to Itself, Revealing Doubts," War on the Rocks, 2019, https://warontherocks.com/2019/02/the-chinese-military-speaks-to-itself-revealing-doubts/.

[30] Hui-jun Wu, "Firmly Grasp the Important Guidelines for National Defense and Army Building [牢牢把握国防和军队建设重要指导方针-国防-浙江在线-浙江潮评论]," Zhejiang News, 2006, http://opinion.zjol.com.cn/system/2006/01/01/006427295.shtml.

[31] "General Secretary Xi Jinping's Important Exposition on the Target of Strong Army [学习习近平总书记关于强军目标的重要论述--理论--人民网]," Guangming Daily, 2013, http://theory.people.com.cn/n/2013/0722/c40531-22275029.html.

[32] Dawei Zhang [张大伟], Di Peng [彭迪], and Yiwen He[和义文], "'A Preliminary Inquiry into How to Solve the Problem of "Five Incapables" Among Commanders' [解决指挥员'五个不会'问题初探]," *National Defense [国防]*, no. 12 (2018): 44–45.

[33] Fangfang Wei [魏方方], Yanfeng Suo [锁延锋], and Jingli Hui [惠景丽], "Analysis and Enlightenment of American Cyber Deterrence Policy [美国网络威慑战略解析及启示]," *Journal of Information Security Research [信息安全研究]* 2, no. 5 (2016): 471–76.

Conversely, looking to the future, the PLA is increasingly composed of university graduates who question the status quo.[34] These recruits were having great difficulty with being integrated into the PLA, mostly being left to support roles.[35] As these new recruits form a more substantial segment over time, it is placed within the realm of possibility that they could make substantial progress in modernizing the military in the future. Such a possibility would allow the PLA to achieve a military capable of joint operations and would be consistent with their expected time frame of 2035[36]. Yet presently, rather than a conventional confrontation using a fully informatized cyber capable army, it currently stands that China seeks to create challenges to American hegemony of the electromagnetic spectrum through asymmetric means.[37]

PLA Cybercommand

These domestic challenges outlined above affects China's standing internationally. For instance, a report by the Economist Intelligence Unit places China at 13th in its overall cyber power rankings, as a measure of its influence in cyber policy matters internationally.[38] The primary source manual of Chinese military thought, the "Science of Military Strategy" in 2013 outlines how American cyber-hegemony remains disconcerting from their point of view.[39] This stems from the reality that institutions in the United States control 10 of the 13 root servers, through which most of the civilian internet is routed. Thus, establishing American control in international cyber policy. China, in forming a diplomatic coalition with Russia has appealed to

[34] Roger Cliff, *China's Military Power* (Cambridge, UK: Cambridge University Press, 2015), https://doi.org/10.1017/cbo9781316217245. 112
[35] Cliff. 114
[36] The State Council Information Office of the People's Republic of China, *China's National Defense in the New Era.*
[37] Berman, *The Logic of Irregular War*.
[38] Economist Intelligence Unit, "Findings and Methodology Cyber Power Index," 2011. 4
[39] Xiaosong Shou, ed., *The Science of Military Strategy* (Beijing: Military Science Press, 2013).

the United Nations to organize a centralized, but multilateral control under the jurisdiction of the UN on multiple occasions.[40] They have used diplomatic means to attempt to pull influence away from and challenge the United States, though it remains a fragile relationship.[41] The available literature in China supports these diplomatic overtures, and pushes for establishing cooperation in cybersecurity with other nations.[42] China perceives the United States as pursuing a similar strategy, particularly in the Asia-Pacific region in order to balance against China.[43]

Whether China has the capability or interest of achieving the status of a major power for the present day in international cyber policy remains to be resolved. For instance, in naval grand strategy China benefits from American command of the seas as its sea lines of communication (i.e. trade including its oil supply, are protected from piracy).[44] In addition, it reveals American capabilities for others to study. In cyberspace, China reaps several benefits from the asymmetry in that increased American presence in the core internet infrastructure confers added vulnerabilities to exploit, as well as opportunities to reconnoiter American capabilities. Conversely the United States is in a much more favorable position to conduct an offensive cyber strategy. This allows China to learn, but it also means they have been left to playing catch-up with American capabilities. The current situation presents China opportunities to steal large

[40] Scott J. Shackelford et al., "Spotlight on Cyber V: Back to the Future of Internet Governance?," Georgetown Journal of International Affairs, 2015, https://www.georgetownjournalofinternationalaffairs.org/online-edition/back-to-the-future-of-internet-governance.

[41] Elias Götz and Camille-Renaud Merlen, "Russia and the Question of World Order," *European Politics and Society* 20, no. 2 (March 15, 2019): 133–53, https://doi.org/10.1080/23745118.2018.1545181.

[42] Cai Cuihong [蔡翠红], "Geopolitics in the Cyberspace: A New Perspective on U.S.-China Relations [网络地缘政治:中美关系分析的新视角]," *The Journal of Internatinal Studies [国际政治研究]* 39, no. 1 (2018): 9–37.

[43] Cai Cuihong [蔡翠红] and Li Juan [李娟], "The US Cybersecurity Cooperation with Asia-Pacific Allies and Its Evaluation [美国亚太同盟体系中的网络安全合作]," *World Economics and Politics [世界经济与政治]*, no. 6 (2018): 51–77.

[44] Ankit Panda, "US Joins Southeast Asia's War on Piracy – The Diplomat," The Diplomat, accessed May 17, 2020, https://thediplomat.com/2014/10/us-joins-southeast-asias-war-on-piracy/.

amounts of data to contribute to its own modernization and development. They have been able to jump ahead multiple generations and forego years of research on account of these efforts in developing the expertise necessary in computer network exploitation.[45]

These issues do not mean that China does not pose any danger to American or Canadian interests. The institutional factors presented shape the types of operations favored by China and lead them to use whatever means that are available to them, at the same time allows them to take advantage of the weaknesses in the infrastructure in North America. As mentioned previously, the Central Military Commission is the highest decision-making body in the PLA, with a top down highly centralized structure. The PLA's cyber command is under the authority of the Central Military Commission, and this allows for the senior members of the Communist Party to sanction and direct cyberespionage efforts.[46] The source of most of these attacks come from a unit designated as Unit 61398.[47]

Through a broad review of the literature it is clear that the Chinese approach has generally favored Computer Network Exploitation (CNE) to conduct reconnaissance, in addition to potentially laying the foundations for future exploitation. Multiple high-profile cases of Chinese CNE have emerged in the past, and many have been reliant on at times unsophisticated social engineering attacks. Two notable examples representative of their efforts being to steal the

[45] William C. Hannas, James Mulvenon, and Anna B. Puglisi, *Chinese Industrial Espionage: Technology Acquisition and Military Modernisation* (New York: Routledge, 2013), https://doi.org/10.4324/9780203630174.
[46] Mandiant, *APT1 Exposing One of China's Cyber Espionage Units* (Alexandria: FireEye Mandiant 2014) 7 https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf.

[47] Mandiant, *APT1*. 7

plans for the C-17 military transport aircraft[48] and the hacking of Equifax.[49] Both of which were carried out with very little manpower, at most requiring three people, and would provide them with increasingly valuable information about American capabilities and American citizens; the latter of which could open the path to increasingly sophisticated attacks and pose new threats to a population now made vulnerable. The modus operandi of Unit 61398 does not tend to be destructive and appears to focus on intellectual property theft.[50] The official stance of the Chinese Communist Party has been to deny such attacks and redirect blame to the United States for alleged "hypocrisy".[51] As such, relying on at times, simple and unsophisticated, but effective means to gather information. These simple means commonly target and are effective against the private sector. primarily falling victim to these attacks. These denials can be explained with the aforementioned manual, the "Science of Military Strategy" from 2013, which foresees that as the practice of using network reconnaissance is already widespread, it is unlikely to be the cause of conflict. As such, China understands the difficulty of responding to such attacks. Nevertheless, they recognize how it could lead the way to attack and sabotage which might escalate.[52]

DPRK comparison

[48] Jules Julien, "How the US Halted China's Cybertheft—Using a Chinese Spy," *Wired*, 2018, https://www.wired.com/story/us-china-cybertheft-su-bin/.
[49] Garrett M. Graff, "China's Hacking Spree Will Have a Decades-Long Fallout," Wired, 2020, https://www.wired.com/story/china-equifax-anthem-marriott-opm-hacks-data/?utm_source=facebook&utm_medium=social&mbid=social_facebook&utm_brand=wired&utm_social-type=owned.
[50] Mandiant, *APT1*.
[51] "Ministry of Defense Spokesperson Geng Yansheng Spoke about the US Department of Justice 's Prosecution of Chinese Soldiers [**国防部新**闻发言人耿雁生就美司法部起诉中国军人发表谈话——**国防部网站**]," Ministry of Defence Network[**国防部网**], 2014, http://www.mod.gov.cn/auth/2014-05/20/content_4510364.htm.
[52] Shou, *The Science of Military Strategy*. 192

The North Korean cybercommand presents a centralized top down structure, similar to the Chinese organization. Under the Reconnaissance General Bureau (one of many competing intelligence services in North Korea) is the Cyber Warfare Guidance Bureau.[53] The title of Guidance Bureau suggests the direct involvement of the Supreme Leader, Kim Jong Un. South Korea is the obvious target for much of these efforts, being at the receiving end of 1.5 million hacking attempts per day.[54] The motivation behind some of these actions demonstrates a clear continuation of the incursions committed by North Korean intelligence agencies over the past century. This plays into the familiar dynamics of provocation between North and South Korea.[55] In studying the attacks conducted by North Korea, the additional motivation of financing the regime emerges, with several attacks having been carried out with the clear motivation of financial gain.

Notwithstanding, several overall considerations carry over from the discussion on China. Where in facing a technologically superior adversary, the North Koreans have resorted to methods exploiting advances in information technology for their information gathering and deterrent signaling. The Korean People's Army (KPA) has a low overall level of modernization, and training in electronic warfare is not widespread across units.[56] The KPA's capabilities are measurably lower than the Chinese PLA in multiple aspects. Thus, the centralization of expertise in the Reconnaissance General Bureau comes as no surprise. Being able to concentrate what few

[53] Jenny Jun, Scott LaFoy, and Ethan Sohn, "North Korea' s Cyber Operations Strategy and Responses" (Washington, DC, 2015), 41
[54] T.W Martin and Jonathan Cheng, "How North Korea's Hackers Became Dangerously Good," The Wall Street Journal, 2018, https://www.wsj.com/articles/how-north-koreas-hackers-became-dangerously-good-1524150416.
[55] Office of the Korea Chair, "Record of North Korea's Major Conventional Provocations since 1960," *Center for Strategic & International Studies* (Washington, DC, 2010), https://www.csis.org/analysis/record-north-korea's-major-conventional-provocations-1960s.
[56] Jun, LaFoy, and Sohn, "North Korea' s Cyber Operations Strategy and Responses." 49

resources they do have, the North Koreans take the training of their cyber experts seriously, recruiting many of their agents from a young age[57].

Deterrence and Attribution

We have sought to establish some of the key observations concerning the behaviour of nations in cyberspace through a broad review of the literature available. Such a review is necessary to explain the behaviour of China given the context of their international and domestic situation. Inasmuch, one of the key difficulties associated with cybersecurity is its impact on the longstanding deterrence assumption. Countries build vast nuclear arsenals with the assumption that this will deter possible threats. It has been suggested that one way to protect from cyberattacks against command and control systems is to tie this to nuclear deterrence,[58] with the same ideas being found in the Chinese literature.[59] This would mean that any cyberattack that meets a threshold of nuclear response would result in nuclear retaliation. However, a propensity to escalate to a nuclear response might not be the most broadly applicable. Furthermore, we are faced with the difficulty of establishing a graduated series of responses to attacks which fall below this nuclear threshold, as our adversaries continue to probe our systems. A cyberattack may fall below the nuclear, or even conventional response thresholds. Illustrative of this, DPRK's cyberattacks on Sony Pictures did not result in a clear response, despite a promise from the Obama administration to do so.[60]

---

[57] Jeremy Laurence, "North Korea Hacker Threat Grows as Cyber Unit Grows: Defector," Reuters, 2011, https://www.reuters.com/article/us-korea-north-hackers/north-korea-hacker-threat-grows-as-cyber-unit-grows-defector-idUSTRE7501U420110601?feedType=RSS.
[58] Defense Science Board, "Resilient Military Systems and the Advanced Cyber Threat" (Washington, DC, 2013).
[59] Tianjiao Jiang, "From Offense Dominance to Deterrence: China's Evolving Strategic Thinking on Cyberwar," Chinese Journal of International Review 1, 2 (2019): 14, DOI: https://doi.org/10.1142/S2630531319500021. 14
[60] Fred Kaplan, Dark: The Secret History of Cyber War (New York: Simon and Schuster, 2017): R502.7, Epub.

Subsequently, the difficulties associated with attributing responsibility are evident in the mode of operation by these external actors. An example of this would be when, in 2012, the personal information of 76 million people was stolen from JPMorgan Chase in a cyberattack. In 2015 it was discovered that the attack was in fact perpetrated by a criminal gang run by two Israelis and an American who operated out of Moscow.[61] Given that the true perpetrators were undiscovered for three years, a militarized or economic response would have resulted in the punishment of an innocent (at least insofar as this specific attack is concerned) target.

Rather than a kinetic response, some such as the commander of USCYBERCOM have proposed the use of easily attributable cyberattacks.[62] These types of attacks could potentially satisfy the necessary conditions of deterrence. This would signal credibility and capability, though it might not be an ideal method.[63] Cyberweapons are for the most part single use. Thus, resorting to easily attributable attacks would become difficult through continuous use as this would allow potential belligerents to patch the flaws that made retaliation possible in the first place. Additionally, it is difficult to determine the impact of a cyberattack from a distance,[64] given that deterrence would require a finer control of response and punishment.[65] Thus, the question becomes, how loud is loud enough? Finally, there is the normative element. Cyberweapons do not necessarily have the same visceral impact as more coercive displays of power. Airstrikes, long range missile attacks, or naval blockades may be viewed as a

[61] Joseph S. Nye Jr, "Deterrence and Dissuasion in Cyberspace," International Security 41, 3 (Winter 2017): 51, DOI: 10.1162/ISEC_a_00266.
[62] Timothy M. Goines, "Overcoming the Cyber Weapons Paradox," Strategic Studies Quarterly 11, 4 (Winter 2017): 87, https://www.jstor.org/stable/10.2307/26271635.
[63] Goines, "Cyber Weapons Paradox," 87.
[64] Matthias Schulze, "Cyber Deterrence is Overrated: Analysis of the Deterrent Potential of the New US Cyber Doctrine and Lessons for Germany's Active Cyber Defence," German Institute for International and Security Affairs 34 (August 2019) 6, DOI: 10.18449/2019C34.
[65] Schultz, "Overrated," 6.

disproportionate response by the international community. Ultimately, it may be that cyberattacks become viewed as routine, much like Soviet aircraft routinely violated American airspace during the cold war.[66]

Case Studies

Operation DarkSeoul

On the issue of capabilities, using a representative example of a North Korean cyberattack, we seek to show how a dyadic rivalry might present itself in the cyber domain. The Korean dyadic rivalry is exceptional as it, has historically included the use of provocative measures, as such, this section will focus on a series sophisticated attacks made against South Korea known as Operation DarkSeoul.

Operation DarkSeoul was a large scale coordinated cyberattack against South Korean media and financial institutions, and it is assumed to be in retaliation for attacks on DPRK government websites, which were blamed on the US and ROK.[67] On March 20, 2013, DarkSeoul created a partial paralysis of the country's financial and media institutions.[68] Overall, approximately 32,000 computers were thought to be affected in the attack.[69] As a result, ATMs, online banking, and computers in media institutions were no longer functioning.[70] Internet banking for Shinhan Bank was blocked, and operations at branches of NongHyup and Jieju

[66] Brandon Valeriano and Ryan C Maness, "The Dynamics of Cyber Conflict between Rival Antagonists, 2001–11," Journal of Peace Research 51, 3 (2014): 358, DOI: 10.1177/0022343313518940.
[67] Choe Sang-Hun, "Computer Networks in South Korea Are Paralyzed in Cyberattacks." New York Times, March 20, 2013. https://www.nytimes.com/2013/03/21/world/asia/south-korea-computer-network-crashes.html.
[68] Kong ji-Young, Lim In Jong, and Kim Kyoung Gon, "The All-Purpose Sword: North Korea's Cyber Operations and Strategies," 9, paper presented at the 11th International Conference on Cyber Conflict: Silent Battle, NATO, 2019.
[69] British Broadcasting Corporation, "North Korea 'behind cyber attack' on South websites," BBC News, July 16, 2013, http://www.bbc.com/news/world-asia-23324172.
[70] Choe, "Computer Networks."

banks were completely disrupted due to the destruction of essential data.[71] The attack used a combination of DDOS techniques and trojans known as Castor and Jokra.[72] These two pieces of malware were used to destroy high value data at both ROK banks and broadcasters. This was accomplished by wiping the master boot record as well as other important files.[73] The malware specifically searched for computers with administrator and root access to servers. Additionally, and somewhat atypically, it was designed to affect multiple operating systems.[74] Perhaps most concerning, they were introduced to their targets through the use of legitimate third-party patches.[75]

While this may have been nothing more than a curious inconvenience for the average South Korean, given that most disruptions were solved within two hours, its strategic significance cannot be overlooked.[76] Firstly, it demonstrates the ability of attackers to disrupt targets remotely and covertly.[77] Secondly, it demonstrated the capacity for long-term planning that was required for such an attack. The attack was setup well in advance, with hackers waiting until 2pm on the 20th to execute it. This assumption is based on the compilation speeds of the wiper malware. Cyber security experts have determined that the malware was compiled several hours before the attack. This would seem to imply that the targets had been infected for at least

[71] Choe, "Computer Networks."
[72] Johnson, A L, "Four Years of DarkSeoul Cyberattacks Against South Korea Continue on Anniversary of Korean War," Broadcom June 26, 2013, https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=edd5c93e-7160-4bf2-a15c-f1c024feb0d7&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments.
[73] United States Computer Emergency Readiness Team (US-CERT), "South Korean Malware Attack," U.S. Department of Homeland Security (April 2, 2013): 1. https://www.us-cert.gov/security-publications/South-Korean-Malware-Attack.
[74] US-CERT "South Korean Malware Attack," 1.
[75] Johnson, A L, "Four Years of DarkSeoul Cyberattacks Against South Korea Continue on Anniversary of Korean War," Broadcom June 26, 2013, https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=edd5c93e-7160-4bf2-a15c-f1c024feb0d7&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments.
[76] Choe, "Computer Networks."
[77] US-CERT "South Korean Malware Attack," 24.

several weeks in advance, as the likelihood that these machines could be infected and destroyed simultaneously in a short timeframe is exceedingly low.[78] Moreover, the attack was found to have similarities with the 2009 Operation Troy attacks in which hackers had exploited a zero-day vulnerability in ROK's military social media network.[79] Thus, DarkSeoul had been at the very least, several years in the making. There is some debate on whether this could be considered an instance of a brandishing cyberattack. Given that no real efforts were made to disguise the origins, the attack could only be described as brandishing given its coordination with other events occurring simultaneously, such as missile tests. The malware used was easily identifiable, and readily tied to the DPRK.[80] Additionally, the malware used in this attack had also been used in previous attacks linked to the DPRK as it traced its lineage back to 2009.[81]

WannaCry

Following the success of operations such as DarkSeoul, North Korea has attempted larger scale attacks, directed not just at South Korea, but the global internet. Therefore, WannaCry has also been selected to demonstrate North Korean hackers' ability to paralyze high value targets, such as government ministries, remotely.

Data destruction and encryption ransomware is a consistent strategy used by North Korean hackers. The WannaCry attacks perfectly illustrate this tendency. In 2017, the attack hit

[78] Dan Goodin "Hard drive-wiping malware that hit South Korea ties to military espionage: "Dark Seoul" attack that wrecked havoc is part of spy campaign operating since 2009," Ars Technica, July 8, 2013, https://arstechnica.com/information-technology/2013/07/hard-drive-wiping-malware-that-hit-s-korea-tied-to-military-espionage/.
[79] Goodin, "Hard drive-wiping malware."
[80] Choe, "Computer Networks."
[81] Dissecting Operation Troy: Cyberespionage in South Korea by McAffee; Kong, In, and Kim, "The All-Purpose Sword" 10.

networks all over globe, ultimately infecting systems in 164 different countries.[82] Unlike DarkSeoul, it had a far wider selection of targets. Indeed, targets ranged from FedEx, the Russian ministry of Interior, the Brazilian social security agency, and 16 British hospitals and clinics. The latter target resulted in cancelled surgeries and a large-scale rerouting of ambulances. Overall, WannaCry affected 300,000 computers worldwide.[83] The worm originally gained access to networks through email phishing attacks. After infecting a system, it would spread to unpatched computers on the network.[84] WannaCry follows the DPRK's approach of sponsoring hacking groups, in this case Lazarus.[85] Thus, its chief purpose was to extort the owners of infected systems, accepting money in the form of Bitcoin with the promise of restoring the encrypted data[86]. While the chief aim was financial, this type of attack has the potential to create chaos in a society and deal damage to its networks. WannaCry did not have the brandishing coordination of DarkSeoul, but its reach was far greater and in many cases its effects took far longer than two hours to resolve.

Russian Cases

This section will perform a cursory review of two Russian cyberattacks with the aim of exposing possible Chinese usages of cyberweapons and warfare. Russia may have a different approach and doctrine, however as it is currently one of the only examples of civilian cyber-mobilization and combined arms, any analysis would be incomplete without its inclusion.

[82] Christopher C. Krebs, "The Response to North Korea's WannaCry Attack Shows Collective Defense Works," Opinion, CNN, December 20, 2017, https://www.cnn.com/2017/12/19/opinions/wanna-cry-and-north-korea-collective-defense-opinion-krebs/index.html.
[83] Scott E. Jasper, "North Korea's Cyberspace Aggression," International Journal of Intelligence and Counterintelligence 31, 1 (2019): 194, DOI: 10.1080/08850607.2018.1524247.
[84] Emma Chanlett-Avery et al., North Korean Cyber Capabilities: In Brief (Congressional Research Service, 2017) 5.
[85] Chanlett-Avery et al., North Korean Cyber Capabilities, 5.
[86] Jasper, "Cyberspace Aggression," 194.

War against Georgia

One the most significant Russian cyber campaigns is the 2008 campaign against Georgia. The campaign began with a DDoS attack against news sites, effectively cutting Georgia off from outside information.[87] Much Like DarkSeoul, one of the key targets were media, and financial institutions. In this case it was not just domestic media that was targeted but also international media such as the BBC and CNN.[88] Additionally, Georgian hacker websites were targeted to ensure that it would be difficult to levy the computer experts in Georgia as a response.[89] While it may seem that these attacks did not serve a direct military purpose, there is evidence of conventional and cyber combined arms efforts. For instance, hackers disabled the websites of companies renting diesel-powered generators in conjunction with conventional strikes against Georgia's electric network.[90] Unlike DarkSeoul, the attacks were not carried out by computer experts trained by the state, but rather by civilians not directly linked to the Russian government and military.[91] Those coordinating the assaults are thought to have been connected to organized crime, and they had been given information on timing and targets in advance.[92]

The goals of this campaign were twofold, the first being control of information surrounding the conflict, the second being the crippling of key infrastructure. If Georgian media and communications systems ceased functioning, then the only narrative would be the Russian one. Thus, Russia was able to cloak its invasion in the normative language of anti-genocide and

[87] Paulo Shakarian, "The 2008 Russian Cyber Campaign against Georgia," Military Review 91, 6 (November-December 2011): 63.
[88] Shakarian: "2008 Russian Cyber Campaign," 64.
[89] Shakarian: "2008 Russian Cyber Campaign," 64.
[90] Shakarian: "2008 Russian Cyber Campaign," 66.
[91] John Bumgarner and Scott Borg, "Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008," U.S. Cyber Consequences Unit (August 2009): 2, http://www.cyberconflict.org/repository/history-of-cyber-and-attacks/incidents-attacks/US-CCU%20Georgia%20Cyber%20Campaign%20Overview.pdf.
[92] Bumgarner and Borg, "Overview," 3.

minority protection.[93] Creating as much confusion and economic damage as possible by taking down the banking and mobile cellphone networks, as well as flooding the leadership with spam emails to make coordination difficult,[94] in conjunction with the securing of ports, railways, and fossil fuel facilities.[95] All information coming in and out of the country was taken over.

Estonia

The cyberattack on Estonia was related to Estonian-Russian ethnic tensions. Much like in Georgia, the attacks were low in sophistication but high in effectiveness. DDoS attacks targeted Estonian infrastructure such as government and political party websites, banks, and the parliamentary email server were disabled.[96] This was achieved through transnational mobilization, being joined by web forums to coordinate the attack. Modern communications enabled people living in different countries but sharing an identity to mobilize.[97] Estonia is a particularly exposed state, its networks facilitate its electric, banking, and utilities services. Almost all bank transactions occur over the internet and its government operates almost entirely digitally.[98]

The Estonian case is one that emphasises the difficulty of deterrence as it relates to cyberattacks, given that Estonia is a NATO state and a conventional attack could trigger Article 5. Furthermore, Russia and Europe are inseparably tied economically, with much of the

[93] Ronald J. Deibert, Rafal Rohozinski and Masashi Crete-Nishihata, "Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia-Georgia War," Security Dialogue 43, 1 (2012): 9, DOI: 10.1177/0967010611431079.
[94] Shakarian: "2008 Russian Cyber Campaign," 64-66;
[95] Bumgarner and Borg, "Overview," 7-8.
[96] Stephen Herzog, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses," Journal of Strategic Studies 4, 2 (Summer 2011): 50-51, DOI: http://dx.doi.org/10.5038/1944-0472.4.2.3.
[97] Herzog, "Estonian Cyber Attacks," 50-51.
[98] Herzog, "Estonian Cyber Attacks," 51.

continent's energy supply either originating in Russia or passing through Russian pipelines.[99] Similarly, given that the West and China are similarly economically linked, it is difficult to effectively deter cyberattacks even with the existing structure in place.

Analysis:

The various case studies of North Korean and Russian approaches to cyberwarfare strategies lead us to several important takeaways. The cases studied here, in addition to the other instances of the use of computer network operations, present a broad range of sophistication and capabilities. Given that cyber conflict is a relatively new presence in the strategic considerations of nations, the behavior of said nations in cyberspace in the context of crises remains uncertain.

It has been theorized that dyadic enduring rivalries have in general shown restraint from partaking in cyberattacks, which might explain the relatively low number of overall cyberattacks.[100] Even the case of North and South Korea presents a relatively restrained rivalry, when compared to the potential for more damaging attacks. Moreover, the dynamics of response and escalation in the cyber domain remains complex and uncertain. As a result, we must study the strategic consequences of cases such as the ones presented in this paper, in order to better understand how far actors are willing to go, and what baseline level of activity countries are willing to tolerate.

As a response to either increasing sanctions or trade tensions, there might be an increase in computer network operations activity as a retaliation from China. As North Korea has been hit with sanctions and gradually excluded from the international community, it could fall within the

[99] Herzog, "Estonian Cyber Attacks," 53.
[100] Valeriano and Maness, "Dynamics,"

realm of possibility to see an increase in cyber-coercive behavior originating from China against financial institutions in the west if such measures were to be replicated. In the extreme case, of continued and rising tensions, an attack on a large scale could temporarily disable the ability of creditors to make loans or sabotage the flow of trade in the stock markets, which would result in significant economic damage.

China sees a broad-spectrum attack, including on civilian infrastructure during a conflict, or in case of a threat to internal stability, as permissible.[101] If tensions were to rise, the ambiguity of attribution inherent to cyberattacks is embraced by the Chinese literature, which seeks to also establish an ambiguity of intention in its escalation signaling.[102] Data destruction efforts in the style of WannaCry or more recent attacks against the ROK defense agency, could be used to attack government departments and health care facilities. Disrupting its adversaries' medical systems and severing contact with the outside world in the form of media and telecommunications is destined to have a psychological effect.

This form of severe retaliation against computer systems would require a unified civil-military structure allowing for a coordinated response, which might be lacking in China. To achieve diplomatic goals by means of cyber-coercion, there must be a unified coherent message. Considering that the only point of civil-military coordination comes from what the PLA perceives the party line to be, as well as the direction of the Central Military Commission (CMC),[103] projections of capabilities by the PLA might fall short. Though as Unit 61398 is primarily directed by the CMC, cyberattacks could potentially be more closely coordinated to be

[101] Shou, *The Science of Military Strategy*.
[102] Laird, "War Control: Chinese Writings on the Control of Escalation in Crisis and Conflict." 10
[103] Scobell, Saunders, and Jones, *PLA Influence on China's National Security Policymaking*.

in line with the party line. Though when placed within the overall context of the military capabilities of the PLA, any response by the PLA to such an escalation of tensions would be lacking. Furthermore, the CMC might not have the expertise to fully take advantage of the cyber-coercive potential at hand. The additional factors of a relatively low digital literacy of the majority of the population leaves them vulnerable to reciprocated attacks from abroad.[104]

There have been recorded instances of North Koreans living abroad in countries such as Mozambique and Indonesia, conducting cyberattacks.[105] Comparably, Unit 61398 has also shown to possess considerable assets abroad, such as servers and including within the United States.[106] This renders attribution as well as prevention difficult. Though this would indicate a well-organized, and evidently capable organization, the methodology of some of the attacks appear to be primitive, reliant on human error. For instance, the social engineering attacks by which the PLA had stolen the plans for the C-17 transport aircraft, were the result of one error made by an employee at Boeing.[107] Conversely, the culprit was caught through sloppiness and human error on their part.[108] Interestingly, the North Korean Cyber Warfare Guidance Bureau have appeared to be bolder in their behavior and have used more sophisticated as well as destructive attacks as was described in the case study of WannaCry. These methods included exploiting the use of

[104] Klaus Schwab, "Insight Report: The Global Competitiveness Report 2018" (Geneva, 2018).
[105] Priscilla Moriuchi, "North Korea's Ruling Elite Adapt Internet Behavior to Foreign Scrutiny" (Somerville, MA, 2018), https://go.recordedfuture.com/hubfs/reports/cta-2018-0425.pdf. 9
[106] Mandiant, *APT1*, 49
[107] Julien, "How the US Halted China's Cybertheft—Using a Chinese Spy."
[108] Julien.

sleeper agents in South Korea,[109] and digitally infiltrating multiple prominent software companies in South Korea.[110]

With the lessons taken from Russian efforts in Georgia and Estonia; we could infer that even if China were to use methods low in sophistication it could still be high in its effectiveness. Should a partial concentration of its available civilian technical expertise be leveraged, in the same manner Russia has, it could result in a constant bombardment of cyberattacks against major US and western media, banks, government servers, and websites. Attacks which would be difficult to defend against, as it is drawn not only from within Unit 61398 but also from Chinese speaking web users living. It also grants China the ability to distance itself from such a cyberattack as it would be difficult to prove direct involvement. Literature in China acknowledges the need of establishing a militia force capable of network operations, yet difficulties in organizing such a force remains.[111] Through experience, China has relied on civilian hackers in appealing to nationalist sentiments in response to discrimination against ethnic Chinese abroad.[112] Yet this is a far cry from a capable, sophisticated cyber-force.

The past lessons of the sources of military effectiveness can prove valuable in explaining the factors which go into establishing a robust and safe internal network security environment. Unit performance on the battlefield is dependent on multiple factors, though one study by

[109] Choe Sang-Hun et al., "Focus Turns to North Korea Sleeper Cells as Possible Culprits in Cyberattack - The New York Times," New York Times, 2017, https://www.nytimes.com/2017/05/16/world/asia/north-korea-cyber-sleeper-cells-ransomware.html.

[110] Ryan Sherstobitoff, Itai Liba, and James Walter, "Dissecting Operation Troy: Cyberespionage in South Korea" (Santa Clara, CA, 2018).

[111] Fu Zhong [钟孚] and Renlong Zhang [章仁龙], "Issues to Be Considered in Developing Militia Cyber Elements [民兵网络分队建设需关注的问题]," *National Defense [国防]*, no. 11 (2019): 64–66.

[112] WIlliam Howlett, "The Rise of China's Hacking Culture: Defining Chinese Hackers" (California State University, San Bernardino, 2016), https://scholarworks.lib.csusb.edu/etd/383.

Beckley shows that the level of economic development might be a good indicator in predicting battlefield performance. [113] Economic development inherently measures for other factors such as human capital and material capabilities, and also it crucially measures institutional maturity. As a result, it could provide a good measure of military effectiveness. In the building of a secure network, all of the human capital and material capabilities which form the network will inherently define the security environment, mirroring the sources of military effectiveness. The most appropriate indicator of this would be the multiple examples of intrusions into the US Department of Defense networks being promptly found and mitigated.[114] This demonstrates an example of institutional maturity in establishing an appropriate security framework. Conversely, how the PLA views itself as potentially vulnerable to cyberattacks is representative of a military in a developing country.[115] This vulnerability is further made evident by the disparity in capabilities across services, and the uneven distribution of capabilities.

Conclusion

Evident shortcomings in the institutional factors of the Chinese military illustrate the difficulties of building a force capable of challenging more technologically advanced armies. As we face new threats enabled by rapidly advancing technological progress, we can look to the lessons from the past in nuclear deterrence and civil defense to help defend the vulnerable population.[116] Just as with nuclear deterrence, it was through brinkmanship crises such as the

[113] Michael Beckley, "Economic Development and Military Effectiveness," *Journal of Strategic Studies*, 2010, https://doi.org/10.1080/01402391003603581.
[114] Fred Kaplan, *Dark Territory: The Secret History of Cyber War* (New York: Simon and Schuster, 2017)
[115] Michael S. Chase, Jeffrey Engstrom, Tai Ming Cheung, *et al.*, *China's Incomplete Military Transformation: Assessing the Weaknesses of the People's Liberation Army (PLA)* (Santa Monica, CA: RAND Corporation, 2015), https://www.rand.org/content/dam/rand/pubs/research_reports/RR800/RR893/RAND_RR893.pdf. 116
[116] David W. Barno and Nora Bensahel, "Defending the Cyber Nation : Lessons from Civil Defense," War on the Rocks, 2015, https://warontherocks.com/2015/06/defending-the-cyber-nation-lessons-from-civil-defense/.

deterrence in the cyber domain has been fully understood, our adversaries will continue to find ways to exploit our vulnerabilities, hoping to compensate for their own.

Bibliography:

Barno, David W., and Nora Bensahel. “Defending the Cyber Nation: Lessons from Civil Defense.” War on the Rocks, 2015. https://warontherocks.com/2015/06/defending-the-cyber-nation-lessons-from-civil-defense/.

Barno, David W., and Nora Bensahel. “Defending the Cyber Nation : Lessons from Civil Defense.” War on the Rocks, 2015. https://warontherocks.com/2015/06/defending-the-cyber-nation-lessons-from-civil-defense/.

Beckley, Michael. “Economic Development and Military Effectiveness.” *Journal of Strategic Studies*, 2010. https://doi.org/10.1080/01402391003603581.

Berman, Ilan. *The Logic of Irregular War*. Lanham: Rowmand & Littlefield, 2017.

Blasko, Dennis J. “The Chinese Military Speaks to Itself, Revealing Doubts.” War on the Rocks, 2019. https://warontherocks.com/2019/02/the-chinese-military-speaks-to-itself-revealing-doubts/.

Bumiller, Elisabeth, and Michael Wines. “China Tests Stealth Fighter as Gates Visits.” The New York Times, 2011. https://www.nytimes.com/2011/01/12/world/asia/12fighter.html.

Cheng, Dean. “Chinese Lessons from the Gulf Wars.” In *Chinese Lessons from Other Peoples ’ Wars*, edited by Andrew Scobell and Roy Kamphausen, 153–200. Carlisle, PA: Army War College Press, 2011.

Cliff, Roger. *China’s Military Power*. Cambridge, UK: Cambridge University Press, 2015. https://doi.org/10.1017/cbo9781316217245.

Cooper, Cortez A. III. *PLA Military Modernization: Drivers, Force Restructuring, and Implications*. Santa Monica, CA: RAND Corp., 2018. https://doi.org/10.7249/ct488.

Cuihong [蔡翠红], Cai. “Geopolitics in the Cyberspace: A New Perspective on U.S.-China Relations [网络地缘政治:**中美关系分析的新**视角].” *The Journal of Internatinal Studies [**国**际政治研究]* 39, no. 1 (2018): 9–37.

Cuihong [蔡翠红], Cai, and Li Juan [**李娟**]. “The US Cybersecurity Cooperation with Asia-Pacific Allies and Its Evaluation [**美国**亚太同盟体系中的网络安全合作].” *World Economics and Politics [**世界**经济与政治]*, no. 6 (2018): 51–77.

Defense Science Board. “Resilient Military Systems and the Advanced Cyber Threat.” Washington, DC, 2013.

Dong [**董子峰**], Zifeng. *The Transformation of Combat Effectiveness [战斗力生成模式转变]*. Beijing: 军事科学出版社, 2012.

Economist Intelligence Unit. “Findings and Methodology Cyber Power Index,” 2011.

Guangming Daily. “General Secretary Xi Jinping’s Important Exposition on the Target of Strong Army

[学习习近平总书记关于强军目标的重要论述--理论--人民网],” 2013. http://theory.people.com.cn/n/2013/0722/c40531-22275029.html.

Götz, Elias, and Camille-Renaud Merlen. “Russia and the Question of World Order.” *European Politics and Society* 20, no. 2 (March 15, 2019): 133–53. https://doi.org/10.1080/23745118.2018.1545181.

Graff, Garrett M. “China’s Hacking Spree Will Have a Decades-Long Fallout.” Wired, 2020. https://www.wired.com/story/china-equifax-anthem-marriott-opm-hacks-data/?utm_source=facebook&utm_medium=social&mbid=social_facebook&utm_brand=wired&utm_social-type=owned.

QQ News. “Guo Boxiong and Xu Caihou’s Corruption Problem Is Not the Crux of Their Problem [郭伯雄、徐才厚贪腐问题不是他们问题的要害],” 2016. https://news.qq.com/a/20160527/018042.htm?utm_source=The+Sinocism+China+Newsletter&utm_campaign=472b96a287-Sinocism05_30_165_30_2016.

Hannas, William C., James Mulvenon, and Anna B. Puglisi. *Chinese Industrial Espionage: Technology Acquisition and Military Modernisation*. New York: Routledge, 2013. https://doi.org/10.4324/9780203630174.

Heath, Timothy R. “The Consolidation of Political Power in China Under Xi Jinping: Implications for the PLA and Domestic Security Forces.” n.d. https://www.rand.org/pubs/testimonies/CT503.html.

Howlett, WIlliam. “The Rise of China’s Hacking Culture: Defining Chinese Hackers.” California State University, San Bernardino, 2016. https://scholarworks.lib.csusb.edu/etd/383.

Julien, Jules. “How the US Halted China’s Cybertheft—Using a Chinese Spy.” *Wired*, 2018. https://www.wired.com/story/us-china-cybertheft-su-bin/.

Jun, Jenny, Scott LaFoy, and Ethan Sohn. “North Korea’ s Cyber Operations Strategy and Responses.” Washington, DC, 2015.

Kaufman, Alison A., and Daniel M. Harnett. “Managing Conflict: Examining Recent PLA Writings on Escalation Control.” Arlington, VA, 2016.

Kou, Chien Wen. “Xi Jinping in Command: Solving the Principal-Agent Problem in CCP-PLA Relations?” *The China Quarterly* 232 (2017). https://doi.org/10.1017/S0305741017001321.

Laird, Burgess. “War Control: Chinese Writings on the Control of Escalation in Crisis and Conflict.” Washington, DC, 2017.

Laurence, Jeremy. “North Korea Hacker Threat Grows as Cyber Unit Grows: Defector.” Reuters, 2011. https://www.reuters.com/article/us-korea-north-hackers/north-korea-hacker-threat-grows-as-cyber-unit-grows-defector-idUSTRE7501U420110601?feedType=RSS&feedName=internetNews&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+reuters%2FUKInternetNew.

Liang, Qiao, and Wang Xiangsui. *Unrestricted Warfare*. Beijing: PLA Literature and Arts Publishing House, 1999.

Liu, Xuanzun. “PLA Moves to Integrate Techniques, Tactics with New Weapons Systems - Global Times.” Global Times, 2019. http://www.globaltimes.cn/content/1136390.shtml.

Martin, T.W, and Jonathan Cheng. “How North Korea’s Hackers Became Dangerously Good.” The Wall Street Journal, 2018. https://www.wsj.com/articles/how-north-koreas-hackers-became-dangerously-good-1524150416.

McCauley, Kevin. “System of Systems Operational Capability: Key Supporting Concepts for Future Joint Operations.” The Jamestown Foundation, 2012. https://jamestown.org/program/system-of-systems-operational-capability-key-supporting-concepts-for-future-joint-operations/.

Ministry of Defence Network[国防部网]. “Ministry of Defense Spokesperson Geng Yansheng Spoke about the US Department of Justice ’s Prosecution of Chinese Soldiers [国防部新闻发言人耿雁生就美司法部起诉中国军人发表谈话——国防部网站],” 2014. http://www.mod.gov.cn/auth/2014-05/20/content_4510364.htm.

Moriuchi, Priscilla. “North Korea’s Ruling Elite Adapt Internet Behavior to Foreign Scrutiny.” Somerville, MA, 2018. https://go.recordedfuture.com/hubfs/reports/cta-2018-0425.pdf.

Mulvenon, James C. *Professionalization of the Senior Chinese Officer Corps: Trends and Implications*. Santa Monica, CA: RAND Corp., 1997.

Office of the Korea Chair. “Record of North Korea’s Major Conventional Provocations since 1960.” *Center for Strategic & International Studies*. Washington, DC, 2010. https://www.csis.org/analysis/record-north-korea’s-major-conventional-provocations-1960s.

Panda, Ankit. “US Joins Southeast Asia’s War on Piracy – The Diplomat.” The Diplomat. Accessed May 17, 2020. https://thediplomat.com/2014/10/us-joins-southeast-asias-war-on-piracy/.

Sang-Hun, Choe, Paul Mozur, Nicole Perlroth, and David E. Sanger. “Focus Turns to North Korea Sleeper Cells as Possible Culprits in Cyberattack - The New York Times.” New York Times, 2017. https://www.nytimes.com/2017/05/16/world/asia/north-korea-cyber-sleeper-cells-ransomware.html.

Saunders, Phillip, Arthur Ding, Andrew Scobell, Yang N.D., and Joel Wuthnow, eds. *Chairman Xi Remakes the PLA: Assessing Chinese Military Reforms*. Washington, DC: National Defense University Press, 2019.

Schofield, Julian. *Militarization and War*. New York, NY: Palgrave Macmillan, 2007.

Schwab, Klaus. “Insight Report: The Global Competitiveness Report 2018.” Geneva, 2018.

Scobell, Andrew, Phillip Saunders, and Seth Jones. *PLA Influence on China’s National Security Policymaking*. Stanford, CA: Stanford University Press, 2015. https://doi.org/10.7249/cb550.

Shackelford, Scott J., Enrique Oti, Jaclyn A. Kerr, Elaine Korzak, and Andreas Kuehn. “Spotlight on Cyber V: Back to the Future of Internet Governance?” Georgetown Journal of International Affairs, 2015. https://www.georgetownjournalofinternationalaffairs.org/online-edition/back-to-the-future-of-internet-governance.

Sherstobitoff, Ryan, Itai Liba, and James Walter. “Dissecting Operation Troy: Cyberespionage in South Korea.” Santa Clara, CA, 2018.

Shou, Xiaosong, ed. *The Science of Military Strategy*. Beijing: Military Science Press, 2013.

Steinbruner, John. *The Cybernetic Theory of Decision*. Princeton, NJ: Princeton University Press, 1974.

The State Council Information Office of the People's Republic of China. *China's National Defense in the New Era.* Beijing: Foreign Language Press, 2019.

Wei, Fangfang [**魏方方**], Yanfeng [锁延锋] Suo, and Jingli [**惠景**丽] Hui. "Analysis and Enlightenment of American Cyber Deterrence Policy [**美国网**络威慑战略解析及启示]." *Journal of Information Security Research [信息安全研究]* 2, no. 5 (2016): 471–76.

Wu, Hui-jun. "Firmly Grasp the Important Guidelines for National Defense and Army Building [**牢牢把握国防和**军队建设重要指导方针-**国防**-**浙江在**线-**浙江潮**评论]." Zhejiang News, 2006. http://opinion.zjol.com.cn/system/2006/01/01/006427295.shtml.

Zedong, Mao. *Problems of War and Strategy*. Beijing: Foreign Language Press, 1960.

Zhang [张大伟], Dawei, Di Peng [**彭迪**], and Yiwen He[**和**义文]. "'A Preliminary Inquiry into How to Solve the Problem of "Five Incapables" Among Commanders' [**解决指**挥员'**五个不会**'问题初探]." *National Defense [国防]*, no. 12 (2018): 44–45.

Zhong [钟孚], Fu, and Renlong Zhang [**章仁**龙]. "Issues to Be Considered in Developing Militia Cyber Elements [**民兵网**络分队建设需关注的问题]." *National Defense [国防]*, no. 11 (2019): 64–66.