Interpreting China's Pursuit of Cyber Sovereignty and its Views on Cyber Deterrence

Major Michael Kolton

INTRODUCTION

On December 31, 2015, Chinese officials announced a substantial reorganization of the armed forces. [1] The reforms cut across the entire People's Liberation Army (PLA),[2] and constitute the most dramatic reorganization of China's armed forces since the 1950s. [3] President Xi Jinping described the reforms as essential for modernizing the military. [4] and the reorganization affirmed the PLA's fidelity to the Chinese Communist Party (CCP). [5] The reform also established a new service branch called the Strategic Support Force (SSF) on par with the Army, Navy, Air Force, and Rocket Force. Among its many missions, the SSF secures electromagnetic space and cyberspace. [6] China's military pundits lauded the SSF as necessary for twenty-first century warfare. [7] For years, the PLA has fielded cyber capabilities at various levels of command, and the SSF elevates control of cyber operations to the highest echelons. [8] Ultimately, the PLA employs cyber forces to ensure cyber sovereignty *(wangluo zhuquan)* and safeguard the *Chinese Dream* across all domains.

This paper examines China's military cyber activities in three parts. First, the paper attempts to identify China's strategic objective in cyberspace. Second, it outlines one interpretation of China's cyber strategy. Finally, the paper explores the efficacy of US cyber deterrence given China's cyber strategy. PLA cyber doctrine remains abstruse, and public literature does not offer a stand-alone cyber strategy document that articulates the purpose of Chinese cyber operations. Leveraging PLA texts and other publicly available literature, this paper offers one possible reading of China's cyber strategy. In the end, the paper highlights some implications for US-China cyber relations and encourages efforts to build mutual understanding on both sides of the Pacific.

Michael Kolton is a US Army major currently assigned as a graduate student at Yale University's Jackson Institute for Global Affairs. He is a US Army Foreign Area Officer (FAO) specializing in China. Prior to his current specialty, Major Kolton served as an infantry officer with deployments to Iraq and Afghanistan. He holds a master's degree in economics from the University of Hawaii at Manoa and a Bachelor's degree in economics from the United States Military Academy at West Point, New York.

PART 1: CYBER SOVEREIGNTY

Based upon a review of public statements and documents, China's cyber strategy appears determined to achieve cyber sovereignty; this end unifies the country's cyber activities. Dr. Lü Jinghua of the Center on US-China Defense Relations at the PLA Academy of Military Science's (AMS) describes cyber sovereignty as the foundation for a new international code of conduct for cyberspace *(wangluo kongjian xingwei zhunze)* in which the principle of sovereignty enshrined in the UN Charter extends to cyberspace.[9] At the 2012 World Conference on International Telecommunications, China and a majority of attending countries advocated for national governments to boost their control of the Internet.[10] The US and its allies foiled this campaign and upheld the status quo multistake holder approach, which invites participation from civil society, private enterprise, national governments, and international organizations. This conflict of ideas remains an ongoing geopolitical dispute that will define the future of cyberspace.

While the US and others applaud freedom on the Internet, the CCP worries about its latent power to destabilize social and political order.[11] When Chinese academic researchers examined the use of social media to organize street protests in Iran and China's Xinjiang, they concluded the US will leverage such technologies to spur regime change in other countries.[12] To mitigate these types of perceived Internet risks, China's Great Firewall blocks sites like Google, Facebook, Twitter, and YouTube.[13] In March 2016, Chinese authorities increased efforts to shutdown virtual private networks (VPNs) that enable citizens and foreign residents to bypass censors.[14] The US government deems an open Internet that transcends national boundaries essential for freedom and prosperity. Yet, Beijing balks at Washington's ideals, and Chinese officials consistently slate US policies on cyberspace governance. There is little reason to believe Beijing will compromise on cyber sovereignty because it seeks unrivaled CCP authority over its citizens in the virtual world.[15]

China's displeasure with the status quo of Internet governance

China's vision for cyber sovereignty imagines cyberspace as a new world for nations to stake their claims. In February 2016, the CCP central committee labeled cyberspace the new frontier of the modern state *(xiandai guojia de xinjiangyu)* and a new arena for global governance *(quanqiu zhili).*[16] Deputy Director of the PLA's National Defense University (NDU) Colonel Li Minghai argues controlling cyberspace *(zhangwo zhi wang quan rutong)* is the twenty-first century equivalent of controlling the maritime domain in the eighteenth century or controlling the air domain in the twentieth century.[17] Colonel Li's historical analogy summons a powerful memory among Chinese readers. British dominance of the high seas allowed European powers to subjugate the Qing Dynasty, and many Chinese citizens still chafe under US Navy patrols of global sea-lanes—especially the South China Sea. Given China's collective trauma from past imperialism, the PLA will not allow history to repeat in cyberspace; it will defend China's sovereignty in the cyber domain.

The PLA employs cyber forces to ensure cyber sovereignty and safe-guard the Chinese dream across all domains.

For decades, the Internet has relied on US-centric architecture in both a technical and organizational sense. In 1998, "a few individuals, a few private standards bodies, several corporations, and the U.S. Department of Commerce" established the Internet Corporation for Assigned Names and Numbers (ICANN).[18] As a California-based, non-profit entity, ICANN pioneered multistakeholder Internet governance beyond the traditional purview of national jurisdictions.[19] In the multistakeholder model, leaders from civil society, private enterprise, and governments collectively determine the rules of Internet operations, which in turn shape the fundamentals of cyberspace. To fulfill its global mandate as facilitator of a free and open Internet, ICANN adopted a charter with by-laws that promote inclusivity and openness.[20]

Over the years, national governments have objected to the Internet's seemingly US-oriented bias. In 2013, Edward Snowden revealed prolific National Security Agency (NSA) surveillance activities, and countries like Brazil and Germany enacted privacy protections that could undermine the Internet's global interconnectivity.[21] A 2015 pro-government Chinese editorial board ridiculed America's so-called "free flow of information" as a ploy to "gather information from around the world, through legitimate and illegitimate means."[22] China and Russia exploited the global controversy surrounding

NSA surveillance to push their model of Internet governance, which cedes control of key Internet operations to national governments.[23]

In light of China's pursuit of cyber sovereignty, September 2016 may prove to be a decisive point for its cyber strategy. For over a decade, the Department of Commerce's National Telecommunications & Information Administration (NTIA) managed a component of Internet operations under contract with ICANN's Internet Assigned Numbers Authority (IANA).[24] In September, NTIA's contract with IANA expired, and the NTIA transferred IANA stewardship to ICANN.[25] The transition raised concerns about the durability of multi-stakeholder governance. Some experts fear an impotent ICANN untethered from US underwriters could gradually allow national governments to compartmentalize cyberspace and sunset the age of free flowing information.[26]

To mitigate perceived Internet risks, China's Great Firewall blocks sites like Google, Facebook, Twitter, and YouTube.

At the November 2016 World Internet Conference, the Cyberspace Administration of China (CAC) endorsed global Internet rules that respect "national sovereignty in cyberspace." Bruce McConnell of the EastWest Institute interprets "national sovereignty in cyberspace".[27] as a noteworthy evolution away from China's controversial pursuit of cyber sovereignty. He explains, "The new language expresses more clearly the obvious point that states should and will exercise responsibility to make cyberspace safer and more secure within their borders ... it removes the impression that any state should seek hegemony in global cyberspace."[28] In this way, McConnell echoes China's long-standing official position on cyberspace governance. On the other hand, a conciliatory tone does not signal a deviation from China's pursuit of cyber sovereignty. China will likely leverage shifts in governance (e.g. the ICANN handover) to shape cyberspace norms.

The importance of cyberspace in twenty-first century warfare

The spirited debate over Internet governance arises from the strategic importance of cyberspace in the twenty-first century. Some PLA theorists believe information age warfare *(xinxi shidai de zhanzhang)* requires militaries to conduct a new hybrid-form of warfare that combines cyber power and firepower. Accordingly, Colonel Li argues cyberspace operations *(wangluo kongjian zuozhan)* will determine victors on twenty-first century battlefields.[29] Therefore, the argument goes, the PLA must build a joint cyber force ready to fight and win future wars.[30] Cyber operations are critical capabilities for national defense, and the PLA cannot allow foreign powers to define the country's future.[31]

In many ways, cyber capabilities have evolved faster than the frameworks leaders rely on to employ them. On April 5, 2016, Admiral Michael Rogers of U.S. Cyber Command (USCYBERCOM) recommended his organization be elevated to a fully unified combatant command.[32] In December 2016, Congress voted to follow such recommendations when it passed the 2017 National Defense Authorization Act (NDAA).[33] The ongoing evolution of China's SSF and USCYBERCOM demonstrate the nascent state of cyber warfare institutions. Chinese and American views of military deterrence also differ, and divergent theories of cyber warfare underscore the importance of ongoing US-China efforts to build norms of behavior in cyberspace. Today's embryonic military cyber doctrines carry risks of bilateral misunderstandings, especially when militaries operationalize cyber deterrence strategies.

At such a pivotal moment in military affairs, mutual understanding between two of the world's great powers is essential for peace. In December 2015, US and China envoys launched a new cybersecurity dialogue to foster mutual understanding that included discussions about confidence-building measures for deescalating tensions.[34] The dialogue followed the September 2015 summit between Presidents Obama and Xi that promised to ease tensions after a string of high-profile cyberattacks.[35] In March 2016, Obama met his counterpart and reiterated China's responsibility to reduce cyber industrial espionage.[36] On December 7, 2016, Attorney General Loretta Lynch, Homeland Security Secretary Jeh Johnson, and Chinese State Councilor and Minister of Public Security Guo Shengkun co-chaired the third US-China joint dialogue on cybercrime. In its joint summary, the US and China committed to "further solidifying, developing, and maintaining the Dialogue mechanism and continuing to strengthen bilateral cooperation in cybersecurity.".[37] At a minimum, these meetings reveal the importance both countries place on cybersecurity.

> The PLA will not allow history to repeat in cyberspace; it will defend China's sovereignty in the cyber domain.

Both the US and China trumpet the strategic importance of cyberspace. In its 2006 *Quadrennial Defense Review* (QDR), the US military recognized China's ambitions in cyberspace and its increasingly sophisticated cyber capabilities.[38] In 2014, the Pentagon reaffirmed "the importance of cyberspace to the American way of life—and to the Nation's security."[39] Similarly, China's military has recognized security imperatives in cyberspace. In 2006, the PLA Daily called cyberattacks a serious threat to national security. Cyber operations reshape the security environment by eroding traditional, geographical boundaries *(dili shang de fen jiexian).* By 2025, China must therefore seize strategic opportunities *(zhanlüe jiyuqi)* to ensure a stable security environment in which electromagnetic spectrum and cyberspace constitute the "fifth-dimension of the battlefield." This "fifth dimension" trope parallels the US military's concept of the cyber domain,[40] the global manmade realm within the informational environment that adds on to the four physical domains of air, land, maritime, and space.[41]

To convey foundational principles for cyber operations, American and Chinese experts have evoked various analogies to describe the informational environment and articulate military imperatives. For example, American and Chinese military writers have both used "cyber terrain" metaphors to express cyber operations.[42] In such analogies, key cyberspace terrain equates to the proverbial high ground on physical battlefields, which militaries must seize in order to dominate an adversary.[43] For example, Senior Colonel Ye Zheng of AMS calls cyberspace the new high ground *(quanxin zhigaodian)* for national sovereignty.[44]

Some PLA theorists believe information age warfare requires militaries to conduct a new hybrid-form of warfare that combines cyber power and firepower.

Military dominance in cyberspace remains a strategic task for the PLA. To obtain cyber sovereignty, the PLA must identify key terrain for its cyber forces to seize, control, and retain. Deputy army commander of the PLA 16th Group Army, Major General An Weiping, argues the PLA must build cyber forces that can "seize the high ground in military competition and win information-based battles."[45] Major General An views cyberspace as "an important battlefield to obtain the information supremacy and a strategic means to obtain asymmetrical advantages."[46] Across all domains, the general expects to employ cyber operations to safeguard national security.[47] Major General An believes cyber operations like the Stuxnet attack on Iran's nuclear centrifuges necessitate developing China's joint cyber forces.[48] In this way, the SSF is a manifestation of China's anxieties over superior US military capabilities.

Since 2006, both militaries have fielded increasingly sophisticated cyber capabilities while refining policies and doctrine to guide their employment. Amid such a fast-paced evolution in military affairs, adversaries understandably struggle to interpret one another's intentions. The secretive nature of security decision-making further undermines the accuracy of predicting an adversary's intent.[49] Moreover, another country's security decisions occur within its specific cultural context, which further confuses political or military signals between powers.[50] Military doctrine differs between China and the US, and this incongruence in cyber doctrine exacerbates the risk for miscalculations and escalation.

Irreconcilable differences

Although the US and China agree on the importance of cyberspace, they fundamentally diverge on the prerogatives a country should enjoy in the virtual world. The Atlantic

Council's Jason Healey calls this divergence "a bifurcation between east and west" that allows little room for compromise.[51] Testifying before Congress in 2015, Assistant Commerce Secretary Lawrence Strickling defended America's support for multi-stakeholder Internet governance. As head of the NTIA, Strickling implicitly criticized China and Russia for pursuing greater control over the Internet.[52] Beijing rejects the ideal of an open Internet, and it has found likeminded leaders in Moscow.[53] The CCP wants to govern its citizens in cyberspace with the same authority it exercises in the physical realm.[54]

Admittedly, China's cyber sovereignty approach does hold national governments accountable for the behavior of their citizens. Such a direct accountability could incentivize laggard countries to more enthusiastically tackle cybercrime originating from within their borders.[55] Despite this potential benefit, the US believes multistakeholder governance underwrites Internet freedom and protects the innovative ecosystem that drives prosperity. The US rejects China's push for a new multilateral approach.

Today's embryonic military cyber doctrines carry risks of bilateral misunderstandings, especially when militaries operationalize cyber deterrence strategies.

Beijing meanwhile remains firmly opposed to the US position. On December 16, 2015, Xi Jinping called upon the international community to "respect the right of individual countries to independently choose their own path of cyber development and model of cyber regulation and participate in international cyberspace governance on an equal footing."[56] In a not too subtle critique of the US, Xi said, "Existing rules governing cyberspace hardly reflect the desires and interests of the majority of countries."[57] The CCP repudiates cyberspace norms that undermine its authority to govern the Chinese people. Colonel Ye Zheng of AMS explains:

> To achieve cybersecurity requires 'cyber rules.' Rules are the basis of order, and order is the basis of security. The core of cybersecurity is to establish cyber rules and implement them. Without cyber rules, activities in cyberspace will be out of control, cybercrimes will be rampant, and cybersecurity will be harmed. Cyberspace is now in a disordered state because no actions have been taken to develop cyber rules and there is no international consensus about how to work out the rules.[58]

China has long combined political, economic, diplomatic, and military elements to defend its sovereignty.[59] Notwithstanding US and European opposition, China and Russia appear firmly committed to pursuing their goal of cyber sovereignty.[60] US and China cyberspace policy goals likewise appear destined for perennial conflict. Beijing has demonstrated a dogged pursuit of cyber sovereignty despite objections from the US and its allies.

PART 2: CHINA'S PLA CYBER STRATEGY

Before we can identify the PLA's cyber strategy, we must understand the national policy goals that guide China's armed forces. The values of a country shape its vision for cyberspace, which then guides national policy and military strategy. On the first page of its 2015 *Cyber Strategy,* the US military declares, "The United States is committed to an open, secure, interoperable, and reliable Internet that enables prosperity, public safety, and the free flow of commerce and ideas. These qualities of the Internet reflect core American values—of freedom of expression and privacy, creativity, opportunity, and innovation." [61] In China, the chief goals of its 2015 draft national cybersecurity law are (1) ensure cybersecurity, (2) safeguard cyberspace sovereignty, national security, and the public interest, (3) protect the legitimate rights and interests of citizens, legal persons and other organizations, and (4) promote the healthy development of economic and social information. [62] These themes from China's cybersecurity law persist across various official publications. Instead of an open and free Internet, China emphasizes security and sovereignty. The US and China differ in their vision for cyberspace, and their subsequent strategies reflect this divergence.

The Chinese Dream: China's national policy objective

Importantly, the PLA safeguards China's national strategic goal of the "Chinese Dream" *(zhongguomeng).* [63] Soon after becoming party secretary in 2012, Xi described the Chinese Dream as collective rejuvenation—a revival of prosperity, unity, and strength. [64] In a 2015 interview with the *Wall Street Journal,* Xi explained that in order to understand the Chinese Dream "one needs to fully appreciate the Chinese nation's deep suffering since modern times and the profound impact of such suffering on the Chinese minds." [65] Under the custodianship of the CCP, the country pursues the Chinese Dream through resurgent national strength free from foreign interference.

Although the US and China agree on the importance of cyberspace, they fundamentally diverge on the prerogatives a country should enjoy in the virtual world.

In May 2015, China's Ministry of National Defense (MND) published a white paper articulating the country's military strategy. The document reimagined military power and entreated the PLA to abandon its "traditional mentality" focused on land warfare. [66] Major General Chen Zhou described the white paper as call for the PLA to adapt to new political-security realities and build a modern military force. [67] A Chinese commentator called the MND white paper the most transparent report of PLA strategy in thirty years. [68] Yang Yucai, professor of strategy at China's NDU, said the document clearly articulates the country's strategic aims.[69] Anthony Cordesman and Steven Colley of the Center for Strategic and International Studies (CSIS) likewise accept the white paper as a conduit for understanding PLA strategic thinking.[70] Admittedly, such publications judiciously reveal information and fail to confirm which concepts the PLA operationalize and which ones they reject.[71] PLA texts do not necessarily reflect views from the whole of Chinese government.[72] Nevertheless, the MND white paper helps examine PLA strategic thinking.

The PLA is an instrument of military policy in service to the CCP and the state.[73] In this light, the PLA must fulfill its mandate *(lüxing shiming)* as the Party's army,[74] and the armed forces must always obey the Party.[75] Strategic goals *(zhanlüe mudi)* determine military decisions, and leaders design strategy and develop doctrine that serves the CCP.[76] The PLA evaluates success by achieving the CCP's political objectives.[77] For example, the CCP expects the PLA to guarantee "a stable external environment for continued economic development."[78] Major General Chen Zhou, director of the National Defense Policy Research Center at AMS, summarizes PLA ethos with a traditional Chinese axiom: military affairs must comply with the needs of politics, and military strategy must comply with the requirements of the country's political strategy *(junshi fucong zhengzhi, zhanlüe fucong zheng'e).*[79] Thus, military strategy must support simultaneous efforts across the whole of government to achieve the CCP's strategic end state.

The Chinese Dream orients China's government across numerous concurrent efforts. The 2015 Military Strategy explains, "China's armed forces take their dream of making the military strong as part of the Chinese Dream. Without a strong military, a country can be neither safe nor strong."[80] China identifies an advanced military as a strategic means *(zhanlüe shouduan)* for accomplishing strategic ends *(zhanlüe mudi).* As the country aims for the Chinese Dream, the strategic end-state for the PLA can be expressed in three sub-objectives: sovereignty, modernity, and stability.[81] These goals translate into enduring themes for the military: (1) Protect the Party and Safeguard Stability, (2) Defend Sovereignty and Defeat Aggression, (3) Modernize the Military and Build the Nation.[82] To accomplish these ends, the MND assigns its armed forces strategic tasks *(zhanlüe renwu),* which guide the employment of resources to accomplish objectives.

Clearly defining a credible cyber deterrent is quite difficult when norms of cyber behavior remain ill-defined.

Both US and China militaries design strategy to support national policy goals. When outlining and designing strategy, the US military often uses an ends-ways-means heuristic.[83] The US military derives strategic guidance from national leaders and then develops the ways and means to accomplish those *ends.*[84] The PLA shares a similar affinity for designing strategy subordinate to national policy.[85] PLA theater strategy likewise implements national strategy.[86] This paper uses an ends-ways-mean framework to simplify and summarize PLA strategic thinking for an American audience.

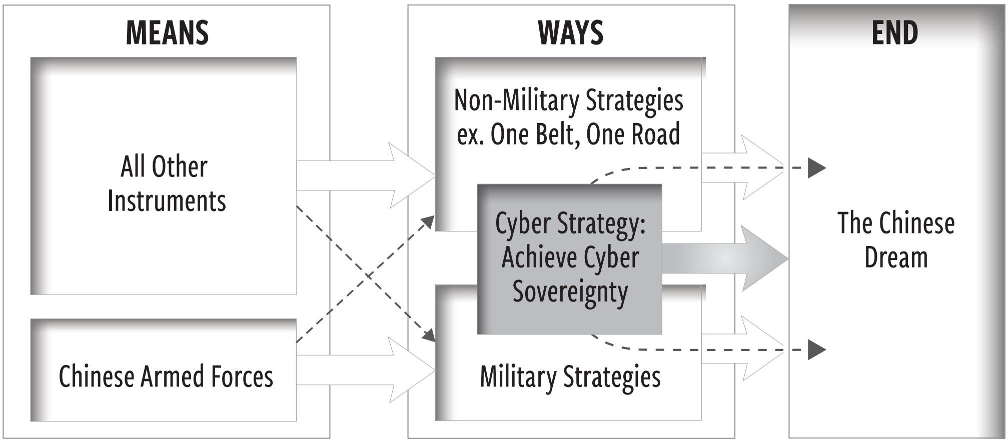

Figure 1: A simplified outline of China's national strategy

In the standard narrative, as China pursues the Chinese Dream, its strategy must meet two decisive milestones called the "two centenaries" *(liang ge yibai nian).*[87] The first centenary occurs in 2021, one hundred years after the CCP's establishment. At that time, China expects to become a moderately prosperous society.[88] The second centenary in 2049 marks one hundred years since the Communists won China's civil war. By this point, China plans to consolidate a "prosperous, strong, democratic, culturally advanced and harmonious" society.[89] In October 2015, the Fifth Plenary Session of the 18th CCP Central Committee reaffirmed the two centenaries in its 13th Five-Year Plan.[90] In an address to the United Nations, Xi identified international stability as one necessary condition for the Chinese Dream.[91] Xi evaluates foreign and domestic policy in terms of achieving the Chinese Dream in step with the two centenaries.[92] Thus, the Chinese Dream and the two centenaries orient and pace the PLA as it operationalizes the national military strategy.

In the cyber domain, leaders have unique *ways* and *means* to pursue objectives. For example, Lieutenant General (retired) Wang Hongguang believes cyber operations enable China to achieve reunification with Taiwan and realize the Chinese Dream without lethal military conflict.[93] The general, a standing committee member of the 12th National Committee of the Chinese People's Political Consultative Conference (CPPCC), argues the PLA must develop sophisticated cyber capabilities to "defeat its adversaries without fighting" *(bu zhan er qu ren zhi bing).*[94] General Wang, a former deputy commander of the Nanjing Military Region, sees cyber capabilities as an asymmetric response to the superior military power of the US and Japan. [95] The general conveys just one of many ways the PLA can leverage cyber operations to achieve strategic *ends.*

Cyber sovereignty: a way to reach the Chinese Dream

To achieve the Chinese Dream, the CCP believes it must secure sovereignty in cyberspace. In 2007, then-President Hu Jintao told Party leaders, "Whether we can cope with the Internet is a matter that affects the development of socialist culture, the security of information, and the stability of the state."[96] Beijing requires internal stability and insulation from external threats to realize the Chinese Dream, and these twin imperatives extend to cyberspace. For example, Lieutenant General Wang Xixin calls for the PLA to employ cyber forces to win future conflicts under the conditions of informationized warfare (xinxihua tiaojian xia kongzhi zhan). [97] In this way, the PLA field's cyber forces to accomplish missions in the information environment, which in turn ensures the CCP achieves cyber sovereignty.

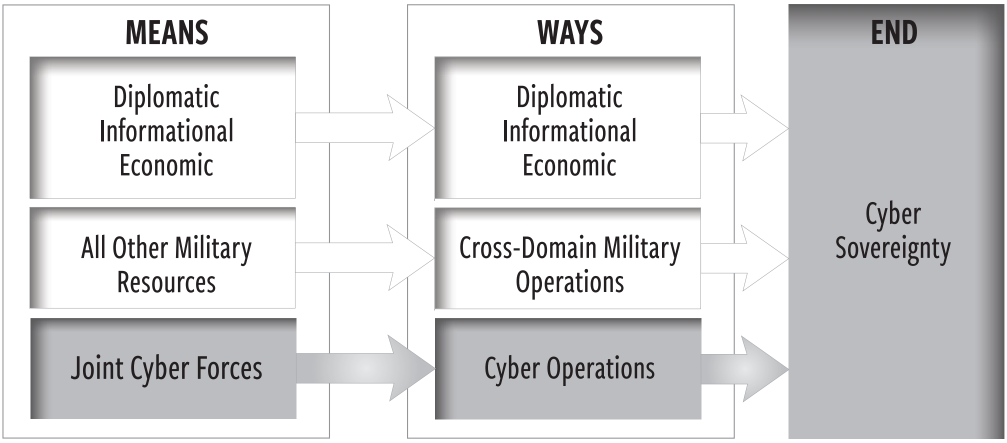
MEANS
Diplomatic Informational Economic
All Other Military Resources
Joint Cyber Forces
WAYS
Diplomatic Informational Economic
Cross-Domain Military Operations
Cyber Operations
END
Cyber Sovereignty

Figure 2: Simplified outline of China's cyber strategy

In 2011, China's pursuit of cyber sovereignty collided with US policy when the White House published its *International Strategy for Cyberspace.* This US policy document promoted an approach to global cybersecurity in accordance with America's "core commitments to fundamental freedoms, privacy, and the free flow of information." [98] China's officials criticized the strategy as a veiled justification for US hegemony in cyberspace. [99] In their analysis, PLA Senior Colonel Ye Zheng and Captain Zhao Baoxian predict the US will pursue cybersecurity with the same self-interest seen in economic and military affairs. Furthermore, the PLA officers expect the US to launch cyber operations whenever necessary to protect its networks *(wuli huwang).* After the Stuxnet attack on Iran's centrifuges, Colonel Ye and Captain Zhao concluded even China's physically isolated networks remain vulnerable to US cyber-attack; passive cyber defense alone is insufficient. Therefore, China must achieve parity with the US in cyberspace to deter aggression and protect national sovereignty. [100]

The 2015 *Military Strategy* affirms the PLA mission to "safeguard China's sovereignty, security and development interests, and provide a strong guarantee for achieving the national strategic goal of the 'two centenaries' and for realizing the Chinese Dream."[101] In the current and future information environment, China considers cyberspace the "new commanding heights in strategic competition" among advanced countries.[102] Although public literature does not offer a stand-alone PLA cyber strategy document, various texts can be summarized through the ends-ways-means framework.[103]

FIGURE 3: THE ENDS-WAYS-MEANS OF CHINA'S CYBER STRATEGY

Ends: Cyber sovereignty; the CCP retains authority in cyberspace and safeguards the Chinese Dream across all domains; China exercises full sovereignty across all domains

Ways:

- Stop and control major cyber crises (e kong wangluo kongjian zhongda weiji)
- Protect national network and information security (baozhang guojia wangluo yu xinxi anquan)
- Safeguard national security and social stability (weihu guojia anquan he shehui wending)
- Support the country's endeavors in cyberspace (zhiyuan guojia wangluo kongjian douzheng)
- Participate in international cyber cooperation (canyu guojia hezuo)

Means: A new joint cyber force (wangluo kongjian liliang jianshe) with the following advanced cyber capabilities:

- Cyber situational understanding (wangluo kongjian taishi ganzhi)
- Cyber defense (kongjian fangyu)
- Precise targeting (jingda quebao weishe)

Major General Chen Zhou explains cyberspace imperatives require China to accelerate cyber situational awareness, cyber defense, the ability to compete in cyberspace, and the ability to collaborate with the international community. With these *means*, China will be able to safeguard national cybersecurity and information security.[104] Similarly, the 2015 *Military Strategy* directs the armed forces to develop the requisite cyber *means* to accomplish assigned tasks. Given this guidance, the PLA must develop doctrine to guide the development and employment of joint cyber forces.

PART 3: US CYBER DETERRENCE

The military doctrine that guides cyber operations has evolved along with cyber capabilities. Do previous paradigms apply in the virtual world? Military theories of airpower and seapower offer one starting point.[105] Nuclear deterrence theory appears helpful in evaluating the interplay of actors armed with devastating weapons.[106] In 2006, the Pentagon endorsed deterrence as a way to dissuade potential adversaries in cyberspace.[107] In December 2015, the White House circulated its cyber deterrence strategy, declaring the US would use "all instruments of national power to deter cyber-attacks or other malicious cyber activity that pose a significant threat to the national or economic security of the United States or its vital interests."[108] The US and China are militarily and economically dependent on cyberspace, and such dependency seemingly guarantees successful mutual deterrence.[109] Yet, deterrence does not dissuade all adversaries,[110] and current US cyber deterrence strategy appears poorly calibrated for deterring China, a resolute and increasingly sophisticated actor in cyberspace.

In many ways, cyber operations and electromagnetic warfare represent quintessential asymmetric threats. Unlike conventional and nuclear weapons, cyber capabilities provide adversaries low-cost military power that targets the vulnerabilities of America's information economy. New America Foundation's P.W. Singer warns, "The problem is that the evidence disproves this link between building up more cyber-offensive capability as the way to scare off the other side. There is not yet any direct pathway to deterrence the way building up nuclear capability yielded it back in the day."[111] If mutual deterrence does not fully translate to cyberspace, the international community must at minimum develop norms that delineate proper cyber behavior.[112] Graham Webster, a Senior Fellow of the Paul Tsai China Center at Yale Law School, writes, "Not every 'cyber' incident is created equal, and retaliation without a clearly communicated principle simply wouldn't deter anything in particular."[113] Clearly established redlines between cyber espionage and cyber warfare, for example, can help reduce the likelihood of unintended escalation.[114]

> Recent US-China interactions in the South China Sea have exemplified the potential for mishap under the compellent form of weishe.

To its credit, the White House appears to appreciate these nuances, and its cyber deterrence strategy seeks international consensus on the "appropriate responses for cyberattacks."[115] President Obama even pushed for an agreement on cyberspace norms at the 2015 G20 summit.[116] This cooperative mindset does not preclude developing" improved defenses, more resilient architectures, and a range of options—cyber and non-cyber—to inflict costs and to hold accountable adversaries that choose to conduct cyberattacks or other malicious activity against U.S. interests."[117] The measured tone of the US cyber deterrence strategy appears to recognize the inherent limits of extending traditional deterrence into the cyber domain.

Nevertheless, the US cyber deterrence strategy has attracted sharp critiques within the US government. Senator John McCain, Chairman of the Senate Armed Services Committee, criticized the White House for failing "to integrate ends, ways and means to meaningfully deter attacks in cyber space."[118] He chastised the report for going "to great pains to minimize the role of offensive cyber capabilities and doing little to clarify the policy ambiguities that undermine the credibility of deterrence."[119] Notwithstanding this feedback, clearly defining a credible cyber deterrent is quite difficult when norms of cyber behavior remain ill-defined.

This high-stakes provocation follows a military weishe approach and reveals a PLA mindset that optimistically assumes American restraint.

Defining deterrence

Military deterrence has long been a pillar of US national security policy in assorted forms across various domains. Yet, such an enduring concept remains ill-defined within US-China relations because the two countries conceptualize deterrence differently. The Pentagon defines deterrence as "prevention of action by the existence of a credible threat of unacceptable counteraction and/or belief that the cost of action outweighs the perceived benefits."[120] Meanwhile, China embeds deterrence within a broader concept of *weishe* that combines deterrence and compellence.[121] In the West, military art distinguishes between deterrence and compellence,[122] but many PLA texts operationalize military *weishe* without clear distinctions between the twin concepts. Even in peacetime, PLA commanders appear to view certain compellent actions as legitimate, while the US and its allies consider them offensive operations.

Western military literature predominantly translates *weishe* as deterrence, but the concept is better interpreted as a particular form of coercion. In his 1966 *Arms and Influence,* Thomas Schelling defined coercion in two parts, deterrence and compellence, and dissected those terms:

> Deterrence and compellence differ in a number of respects, most of them corresponding to something like the difference between statics and dynamics. Deterrence involves setting the stage—by announcement, by rigging the trip-wire,

> by incurring the obligation—and *waiting*. The overt act is up to the opponent. The stage-setting can often be nonintrusive, nonhostile, nonprovocative. The act that is intrusive, hostile, or provocative is usually the one to be deterred; the deterrent threat only changes the consequences *if* the act in question—the one to be deterred—is then taken. Compellence, in contrast, usually involves *initiating* an action (or an irrevocable commitment to action) that can cease, or become harmless, only if the opponent responds. The overt act, the first step, is up to the side that makes a compellent threat. To deter, one digs in, or lays a minefield, and waits—in the interest of inaction. To compel, one gets up enough momentum (figuratively, but sometimes literally) to make the other *act* to avoid collision … Compellence has to be definite: We move, and you must get out of the way.[123]

China's Research Department of Military Strategy defines military *weishe* as a "strategic operation, with the threat to use or the actual use of military capability in order to influence the adversary's strategic judgments by making the adversary feel [that it is too] difficult to achieve anticipated targets or the cost may exceed the benefit."[124] The "actual use of military capability" suggests a broad spectrum of military activities. From benign to dangerous, *weishe* actions increase uncertainty and risk escalation. If Beijing orders military action to compel Washington to change a policy, the operation may unintentionally cross an American redline that then escalates an otherwise manageable dispute.

China appears willing to employ provocative measures to compel a change in US policy and secure its interests in the region.

Recent US-China interactions in the South China Sea have exemplified the potential for mishap under the compellent form of *weishe.* Beijing seeks unchallenged authority over its maritime claims and treats the South China Sea as an issue of sovereignty. Meanwhile, the US Navy operates freely in international waters according to established norms. China interprets US naval operations as a challenge to its national security. In 2009, Chinese white-hulled vessels aggressively maneuvered against the USNS *Impeccable* and nearly caused a collision. In this instance, Beijing used non-military coercion and chanced military conflict to compel a shift in US policy.[125] This high-stakes provocation follows a military *weishe* approach and reveals a PLA mindset that optimistically assumes American restraint.

Numerous PLA theorists have written about warfare in the twenty-first century. Regarding *weishe,* prevailing thought appears to hold "a country should not hesitate to deter through military force if there is no other way to control a crisis."[126] At times, China's deterrence parallels US notions. For example, the PLA expects its state-of-the-art air power to "discourage other countries from conducting air and other military operations against China or to convince any adversary to abandon its own military operations."[127] Yet, the compellence form of *weishe* still resembles US offensive operations. For example, China considers space weapons that target satellites a form of *weishe* at the extreme end of the peacetime continuum, but the US treats such weapons as offensive capabilities for war.[128] This incongruence between US deterrence and China's *weishe* degrades escalation management by fomenting miscues. This US-China doctrinal gap is especially relevant to cyber operations given persistent ambiguity about appropriate behavior in cyberspace.

Although publications often translate *weishe* as deterrence, such expediency encourages an erroneous frame for Chinese actions. This paper therefore retains the term *weishe* when discussing Chinese texts to aid accurate interpretation of Chinese signaling. Summarizing China doctrine, Kevin Pollpeter of UC San Diego's Institute on Global Conflict and Cooperation (IGCC) explains, "Effective coercion [*weishe*] not only requires a strong capability and the will to carry out threats, those threats must be communicated effectively so that the target of the coercion is cognizant of the full costs of coming into conflict with China."[129] The emphasis on signaling requires Washington to understand Beijing's message. Therefore, China must calibrate its message for its intended audience before launching an irrevocable course-of-action. Ultimately, peace between the US and China rests on maturity and mutual understanding.

One unofficial cyber weishe approach

The PLA considers compellent forms of *weishe* legitimate in peacetime. Extending *weishe* to cyberspace meanwhile remains a nascent concept. AMS researcher Yuan Yi proposes one approach for cyber *weishe*. Yuan believes cyberspace is a strategic area with *weishe* opportunities.[130] In the twenty-first century, he argues the PLA must employ cyber operations to achieve *weishe* across all domains. According to Yuan's cyber *weishe* approach, cyber operations must showcase an adversary's impotence in the physical and virtual worlds.[131]

FIGURE 4: YUAN YI'S REQUIREMENTS FOR EFFECTIVE CYBER WEISHE

Build the proper cyber force: Well-organized joint cyber force *(wangluo zhan liliang xingcheng heli)* that can organize and coordinate the power of the network of 'patriotic' hackers *(aiguo heike).*

Select the proper target: Must identify high-value targets that clearly demonstrate China's role because an innocuous attack could be incorrectly attributed to common hackers *(yi bei wu renwei shi putong heike zhizao)* and fail to achieve the desired effect of deterrence. Cyber operations require sophisticated precision *(jing da quebao weishe)* to prove the futility of challenging Chinese interests.

Execute information campaign: Before attack, China must issue a warning to the adversary through extensive propaganda *(yao tongguo guangfan de yunlan xuanchuan zaoshi, xiang diguo fachu daji jinggao).* After attack, ensure adversary recognizes China's superb cyber capabilities *(yi zhanxian jifang gaochao de wangluo gongji jishu he shoudian).*

Yuan's cyber *weishe* approach exceeds the scope of deterrence under US doctrine. Yuan even concedes dangerous uncertainty in his cyber *weishe* proposal because he cannot predict US reactions to aggressive cyber operations.[132] In 2014, Yuan coauthored a piece in a PLA newspaper that rebuked US cyberspace hegemony and called for the mobilization of Chinese citizens to carry out massive cyber-attacks against the US.[133] Yuan presents a highly aggressive perspective in PLA cyberspace thinking. Commenting on Yuan's proposal, CFR's Adam Segal writes, "The article is almost definitely not an authoritative overview of what the People's Liberation Army thinks about deterrence but at the same time it is equally unlikely to be completely outside the mainstream."[134] To marginalize Yuan-like thinking, Segal hopes leaders from both countries will "meet soon, and start the discussion on the meaning of deterrence and other basic concepts."[135] Segal's concerns seem prudent given the risks of escalation a Yuan-like mindset imbues.

A cyber weishe interpretation of the 2014 OPM cybersecurity breach

Prior to the Obama-Xi summit in September 2015, one of the most discussed national cybersecurity topics was the 2014 breach at the US Office of Personnel Management (OPM).[136] Most likely a PLA cyber operation, the OPM breach exposed the sensitive information of nearly 22 million current and former government personnel, contractors, and family members. The impact of the OPM breach continues to reverberate. On February 22, 2016, OPM's chief information officer resigned over the scandal seven months after the OPM's director also departed.[137] In September 2015, the CIA reported the OPM hack forced the Agency to withdraw compromised intelligence officers from the field.[138] US officials described the OPM breach as cyber espionage, and most media coverage cited the intelligence value of the stolen information as an explanation for the breach. The China's government claims the OPM breach was a cybercrime, not state-sponsored espionage.[139] and they even arrested several alleged hackers.[140] Nevertheless, the US intelligence community remains confident the breach was a state-sanctioned cyber operation. By characterizing the event as cyber espionage, the US deemed the breach a case of spying that all governments conduct during peacetime.

Although cyber espionage offers a reasonable explanation for the OPM breach, this paper offers an alternative interpretation. Rather than a matter of spying, the OPM breach appears to be a categorical success under cyber *weishe*. The cyberattack struck a high-value target with very little collateral damage, showcased the sophistication of Chinese cyber forces, compelled US leaders to revisit cybersecurity policies, and signaled

China's willingness to use cyber operations for national security ends. In accordance with military *weishe*, the cyberattack selected a target that generated a tolerable US response. Despite public scrutiny and embarrassment, the Obama administration remained considerably restrained. Admiral Mike Rogers told the Atlantic Council that the OPM breach was part of a significant PLA information collection effort.[141] Director of National Intelligence James Clapper identified China as the likely culprit, but the administration did not escalate rhetoric much further.[142] General (retired) Michael Hayden, former head of the NSA and the CIA, assessed OPM's repository as a legitimate target for cyber espionage.[143] By choosing cyber espionage as opposed to a Stuxnet-like attack, China's leaders astutely kept their cyber operation within the scope of acceptable peacetime activities.

Around the world, emerging military powers are building capabilities that intentionally enhance uncertainty.

The purpose for the OPM breach can be interpreted through the lens of China's cyber strategy, which pursues cyber sovereignty. Thus, the Obama-Xi summit can be seen as a victory for China's cyber sovereignty agenda: two presidents directly discussing a state's duty to govern its citizens and enforce laws in cyberspace. President Obama delivered stern remarks about the need for China's government to curb cybercrime, but the OPM breach did not feature in public discussions.[144] The two presidents agreed that stealing intellectual property undermines the international economic order.[145] In accordance with cyber *weishe*, PLA cyber operations compelled Washington to elevate cybersecurity to the highest levels of diplomacy and partially validate China's arguments for sovereign control in cyberspace governance.

After the Obama-Xi summit, the US intelligence community assessed that PLA cyber operations would continue apace.[146] Xi escaped overt criticism while advancing China's cyberspace agenda. Beijing leveraged the summit to promote its view that only national governments can effectively secure cyberspace. In this way, the OPM breach may have helped compel Washington to partially acquiesce to Beijing's pursuit of cyber sovereignty. In December 2015, US and China envoys launched the cybersecurity dialogue agreed upon during the Obama-Xi summit. Meanwhile, Xi addressed the World Internet Conference and strongly advocated for cyber sovereignty as the future paradigm for Internet governance.[147] Clearly, China continues to pursue cyber sovereignty.

Harvard's Jack Goldsmith also believes Xi used US reaction to China's cybercrime for domestic purposes. Goldsmith points to a precipitous drop in commercial cyber espionage well before the presidential summit in September 2015.[148] Goldsmith interprets changes in Chinese cyber behavior as "less about the U.S. imposing or threatening hefty costs on a unitary China (the costs and threatened costs have not in fact been hefty), and more about the U.S. making transparent corrupt state-sponsored activities to China's government, and thus aiding China's government (as embodied in Xi's regime) in furthering its interests."[149] In this view, the 2015 presidential summit helped Xi consolidate control over cyberspace within China.

In short, cyber operations like the OPM breach should be assessed beyond their intelligence value. When PLA cyber operations are controlled at the highest echelons, such activities merit thorough analysis of second- and third-order effects. This paper argues such cyberattacks aim to compel the US to react in ways that erode the sanctity of an open Internet. If the strategic objective of China's cyber strategy is cyber sovereignty, then the US remains the largest obstacle to China's ambitions to displace the status quo. Thus, in accordance with cyber *weishe*, Beijing will act to undermine multistakeholder cyberspace governance, compel Washington to acquiesce to cyber sovereignty, and galvanize international support for rewriting norms that govern the Internet.

PART 4: DOCTRINAL DIFFERENCES BETWEEN US AND CHINA

Just as the US and China diverge on their understanding of deterrence, the military doctrine of the two countries further aggravates misunderstandings over cyber operations. China expert Gregory Kulacki notes, "PLA strategy is focused on understanding and responding to U.S. investments in the advanced conventional military capabilities it believes the United States intends to use to undermine the credibility of China's overall military deterrent."[150] Consequently, the US-China military relations suffer a feedback loop where the strategic decisions of one country influence the decisions of the other. As US and China strategists estimate the future actions of one another, miscalculation appears inevitable.

As mentioned previously, the South China Sea illustrates opportunities for such misunderstandings. The Naval War College's Peter Dutton argues the "combination of economic leverage, civilian maritime power, and military deterrence power has enabled a Chinese strategy in which there are little or no consequences for the employment of escalation, short of militarized armed conflict.".[151] Dutton identifies a gap between US and China doctrine in which China employs "non-militarized coercion" to achieve strategic objectives.[152] According to Dutton, recent maritime patrols exemplify China's predilection for non-militarized coercion. China's white-hulled vessels outnumber the combined maritime forces (navy and coast guard) of all other South East Asian neighbors. China now exercises "de facto control over much of the disputed water space."[153] From the US perspective, such activities destabilize regional stability, but China's actions align with its tradition of military *weishe*. China appears willing to employ provocative measures to compel a change in US policy and secure its interests in the region.

As cyber capabilities evolve on both sides of the Pacific, US and China cyber operations will intensify the consequences of warfare in the twenty-first century information environment.[154] University of Toronto's Jon Lindsay warns, "The rhetorical spiral of mistrust in the Sino-American relationship threatens to undermine the mutual benefits of the information revolution." [155] Lindsay also writes, "Overlap across political, intelligence, military, and institutional threat narratives makes cybersecurity a challenging policy problem, which can lead to theoretical confusion." [156] In this way, doctrinal confusion can generate misunderstandings with serious consequences.

Doctrine-difference theory

To explore the consequences of doctrinal confusion, Naval Postgraduate School's Christopher Twomey tests "the causal claim that doctrinal differences worsen misperceptions, which can lead to escalation."[157] In one case, he applies doctrinal-difference theory to China's decision to escalate involvement in the Korean War after American-led forces crossed the 38th parallel in October 1950. America's aggressive pursuit of North Korean forces stoked Chinese fears about an anti-communist bloc in Northeast Asia. [158] Beijing could not tolerate a unified anti-communist Korea. By November, tens of thousands of PLA soldiers had entered combat in North Korea. In hindsight Beijing had strongly signaled their interests on the Korean Peninsula well before it entered the war; however, the US failed to recognize the gravity of China's redlines. [159]

On September 7, 1950, the National Security Council concluded, "Although politically unlikely, it is possible that Chinese Communist forces might be used to occupy North Korea ... it is possible that the Soviet Union, although this would increase the chance of general war, may endeavor to persuade the Chinese Communists to enter the Korean campaign." [160] On October 2, the White House authorized General Douglas MacArthur to operate north of the 38th parallel. In months preceding this decision, the PLA had visibly prepared for a Korean contingency. During the summer of 1950, Mao Zedong redeployed troops to Manchuria from their Taiwan-invasion posture in Fujian. For several weeks, PLA infantry formations conducted exercises near the Korean border, signaling China's intent to check a US maneuver northward. On the diplomatic front, strategic dialogue proved wholly insufficient, because Beijing and Washington had not restored diplomatic relations following China's civil war. [161] The two countries failed to retain a mechanism for mitigating tensions or preventing escalation.

Meanwhile, MacArthur and his staff misinterpreted PLA doctrine and underestimated Beijing's commitment to the Korean Peninsula. The US military erroneously assumed its air power would neutralize the PLA. Moreover, MacArthur expected China to commit their main effort near the 38th parallel as the Americans maneuvered across the mountainous terrain. [162] In fact, the main PLA forces were postured much further north. PLA doctrine dictated a "lure them in deep" operational approach that encouraged American forces to extend their supply lines into North Korea's restrictive terrain. [163] As late as December, the US continued to grossly underestimate the massive number of PLA troops it faced. [164]

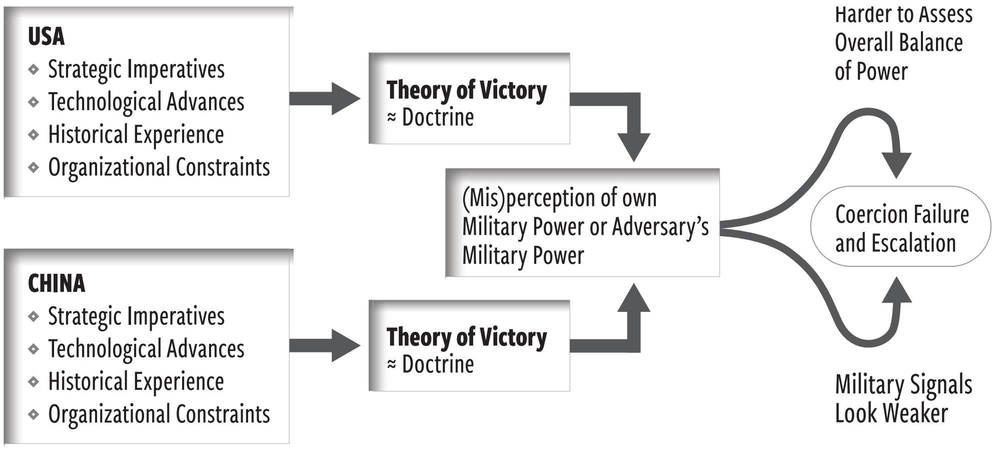
USA
Strategic Imperatives
Technological Advances
Historical Experience
Organizational Constraints
CHINA
Strategic Imperatives
Technological Advances
Historical Experience
Organizational Constraints
Theory of Victory
≈ Doctrine
Theory of Victory
≈ Doctrine
(Mis)perception of own Military Power or Adversary's Military Power
Harder to Assess Overall Balance of Power
Coercion Failure and Escalation
Military Signals Look Weaker

Figure 3: Modified Twomey Doctrinal-Difference Model

The US-China confrontation in the Korean War illustrates "the link between different theories of victory and underestimation of the enemy."[165] Twomey explains, "Differences in theories of victory here directly contributed to U.S. misperception of its adversary's relative capabilities. This suggests that American assessments of the balance of power and of Chinese signals before the war were adversely affected by the misperceptions.".[166] Although the US intelligence assets observed PLA exercises in Manchuria, Washington did not interpret the signals as commitment to intervention. Additionally, MacArthur underestimated the PLA's strength and capabilities.[167] The deterrence aspect of *weishe* failed for China. The divergence between Chinese and American military thinking intensified a war that killed over 36,000 Americans, 1.2 million South Koreans, a million North Koreans, and 600,000 Chinese troops.[168]

Accurately interpreting an adversary's doctrine is necessary for predicting its actions in a deterrence approach. Since *weishe* relies on signaling, misperception of military signals increases the likelihood of a weishe failure and unintended escalation. In 2000, George Washington University's David Shambaugh called PLA doctrine the driving force behind "all other facets of China's military modernization."[169] Hence, the US must accurately understand PLA military theory to ensure national security. Doctrine reveals a military's approach to tactical, operational and strategic decisions; it is the key to deciphering military signals.

PLA doctrine is subordinate to national strategic interests and guides the military's transformation.[170] Similarly, the US military treats doctrine as the foundation for military training and operations.[171] Unlike the US military, the PLA integrate political thought into military decision-making at all echelons.[172] These political imperatives shape training, operations, and strategic design within the PLA. In addition, the PLA operate with a far more asymmetric mindset than the US military.[173] PLA and US military doctrine differs, which shapes their respective military strategy and operations.[174]

Across all domains, accurately evaluating an adversary's doctrine remains fraught with challenges. In cyberspace, the intent behind military activity appears even more obscure. Such uncertainty regarding the purpose of an adversary's cyber operations muddles the taxonomy of threats and undermines the effectiveness of a cyber deterrent. [175] Doctrinal-difference theory warns that today's cybersecurity status quo carries serious risks of doctrinal confusion, coercion failure, and escalation.

A growing military affinity for ambiguity

To prevent unintended war, strategists traditionally reduce ambiguity. Yet, around the world, emerging military powers are building capabilities that intentionally enhance uncertainty. In 2015, US Joint Chiefs of Staff described a new hybrid threat, which "blends conventional and irregular forces to create ambiguity, seize the initiative, and paralyze the adversary."[176] Hybrid conflicts "increase ambiguity, complicate decision-making, and slow the coordination of effective responses." [177] The US military believes future adversaries are pursuing asymmetric capacity for hybrid warfare. [178] The U.S. Army operates under the assumption that "changes in technology and geopolitical dynamics as well as the enduring political and human nature of war will keep war in the realms of complexity and uncertainty."[179] In response to this threat, the US military is investing in technologies and organizational structures that boost agility to respond to unpredictable threats. [180] The US finds it increasingly difficult to prepare for future conflicts.

The US must clearly delineate redlines for cyberspace behavior to prevent PLA cyber operations from unnecessarily provoking a conflict.

PLA military theorists have reached a similar conclusion about twenty-first century warfare. Lieutenant General Wang Xixin predicts China faces an era of low-intensity conflict requiring new operational approaches. [181] The PLA fears "conflict may erupt from a crisis that has spiraled out of control, rather than from an intent to start a war." [182]] PLA Colonel Lin Dong argues China's military thinking remains underprepared for future threats. Interestingly, he also believes the US military practices a form of hybrid warfare (*hunhe zhanzheng*), and the PLA must therefore adopt a new political-military theory that better integrates military strategy with foreign policy. [183] Like the US military, the PLA sees an era of uncertainty that requires careful management to minimize the scale of future crises.

Unfortunately, this era of uncertainty extends to cyberspace. The divergent views of cyber deterrence and cyber *weishe* seem ripe for future conflict. Adam Segal writes, "Beijing and Washington have a common interest in preventing escalatory cyber operations—attacks that one side sees as legitimate surveillance but the other views as prepping the battlefield." [184] Segal recommends, "The two sides could consider conducting formal discussions on acceptable norms of behavior and possible thresholds for use of force as well as greater transparency on doctrine. These cooperative measures can reduce the chance of misperception and miscalculation and thus diminish the likelihood that a conflict in cyberspace will become kinetic."[185] In a security environment wrought with uncertainty, two great powers can ill-afford misinterpretations.

The search for mutual understanding

For years, mutual understanding has been the hallmark of international cyber policy. On December 29, 2009, the United Nations General Assembly adopted a resolution affirming the necessity of cooperation for global cybersecurity.[186] At a 2012 conference with his Chinese counterpart, Secretary of Defense Leon Panetta emphasized the importance of working "together to develop ways to avoid any miscalculation or misperception that could lead to crisis in this area [of cyber defense]."[187] In 2015, US State Department's Michele Markoff emphasized mutual understanding during a panel discussion in Beijing. As the deputy director of the Office of the Coordinator for Cyber Affairs, Markoff encouraged countries to develop "practical cyber confidence building measures" and promote international norms in cyberspace.[188]

Despite espousing mutual understanding, US-China mistrust over cybersecurity remains pervasive. In July 2014, Secretary of State John Kerry and State Councilor Yang Jiechi met in Beijing at the sixth round of the US-China Strategic and Economic Dialogue (S&ED). Among a long list of topics, the strategic dialogue reaffirmed an imperative to "build greater mutual understanding in military-to-military relations through improved communication and contacts at all levels."[189] Reflecting on the S&ED, senior Chinese diplomat Zhou Jingxing assessed, "the insufficiency of strategic mutual trust is the root of all problems between the US and China."[190] Senior Colonel Zhao Zijin and Colonel Zhao Jingfang argue military crises often occur by accident, but the root causes (*baofa genyuan*) are fundamental conflicts of interest between countries and political groups. So long as disputes remain unresolved, they argue, unfortunate incidents can escalate into crises.

Even if disputes remain unresolved, the US and China can still develop mechanisms to deescalate situations. Former assistant secretary of state for East Asian and Pacific affairs Kurt Campbell states, "It is probably inevitable that there is going to be more tension in the relationship between the United States and China going forward. So, learning how to deal with that tension and manage it effectively will be one of our great challenges."[191] Similarly, US Army Brigadier General Kimberly Field and Major Stephan Pikner predict that US-China relations will encounter "points of friction, especially given America's (admittedly intermittent) underwriting of the Responsibility to Protect doctrine that contrasts starkly with China's emphasis on state sovereignty as paramount."[192] The two Army officers advocate "a framework of mutual restraint between the United States and China, in conjunction with a broader engagement strategy."[193] Both Field and Pikner hope to avoid accidental escalation through increased collaboration.

Lauding the September summit, Obama stated, "The candid conversations between President Xi and myself about areas of disagreement help us to understand each other better, to avoid misunderstandings or miscalculations, and pave the way potentially for further progress in those areas."[194] Xi said the two countries must enhance strategic trust, increase mutual understanding, and respect each country's interests. China's president emphasized US-China relations face a single option: win-win cooperation.[195] Despite the proclaimed goal of mutual understanding in cyberspace, the summit produced modest outcomes. [196] Trust remains an aspiration.

Four Recommendations

Ultimately, the goal of US cyber deterrence is to prevent cyberattacks, and current US cyber policy likely deters many threats. With respect to China, the US must clearly delineate redlines for cyberspace behavior to prevent PLA cyber operations from unnecessarily provoking a conflict. The four following recommendation are meant to help promote this goal.

1. **Continue the cybersecurity dialogue:** The Obama-Xi summit directed experts to improve mutual understanding over cybersecurity. These meetings are conduits for developing confidence-building measures and could eventually design mechanisms to deescalate future cyber-related crises. When cyberattacks and retaliation move at light speed, decision-makers must carefully manage escalation.

2. **Produce a Glossary of Cybersecurity Terms:** Written in English and Chinese, experts should produce a comprehensive document that clarifies each government's official stance on cyber operations. The details of this publication should mirror the *United States-Chinese Glossary of Nuclear Security Terms* by the Committee on International Security and Arms Control (CISAC) of the American National Academies of Science (NAS). The cybersecurity working group should produce doctrinal definitions that Chinese and English linguists absolutely concur reflect the intent of both governments. As US-China teams collaborate, they should especially dissect each government's view of cyber deterrence. This challenging exercise could eventually help construct inclusive global norms for cyberspace behavior, which could then boost cybersecurity for all stakeholders worldwide.

3. **Encourage Track 1.5/2 diplomacy addressing cyber deterrence:** Diplomatic channels facilitate valuable dialogue. Current and former US policymakers should meet with their Chinese counterparts to discuss cyber deterrence at various forums like the Shangri-La Dialogue and the U.S. Strategic Command (USSTRATCOM) Deterrence Symposium. US organizations like the Carnegie-Tsinghua Center should invite American and Chinese experts to conferences that address cyber deterrence.

4. **Commission a study of Chinese cyber deterrence for public release:** The Department of Defense should commission an organization like RAND or CNA to produce a report summarizing PLA military thinking on cyber deterrence. The final report should be made public to entice Beijing to critique the interpretation of China cyber policy. CSIS, Brookings, or other think tanks should then invite China's leaders to speak at events and debate the merits of this semi-official report. Through these channels, China officials will feel compelled to clarify ambiguous cyber policies.

These four recommendations require US officials and their partners to sufficiently understand US cyber policy. Specifically, the US must clearly articulate redlines so that current and former officials can accurately convey them to Chinese counterparts. Furthermore, this paper's recommendations rely on Beijing's reciprocity in clarifying their doctrine.

Given the complexity of evolving US cyber policy, interagency cooperation may need to produce a primer that summarizes US cyber policy. Developing interagency consensus such a document offers an opportunity to clarify the ends-ways-means of US strategic thinking on cyberspace. Perhaps this exercise would help identify and rectify inconsistencies across various US agencies and promote unity of effort in cyber defense.

As Beijing pursues cyber sovereignty, it appears willing to use cyber operations to compel the US to reorient its cyber policy. The US cyber deterrence strategy rightly promotes international cooperation, public-private partnerships, multi-stakeholder governance, and critical infrastructure protection. On the other hand, the cyber deterrence strategy also intentionally promotes "uncertainty in adversaries' minds about the effectiveness of any malicious cyber activities and to increase the costs and consequences that adversaries face as a result of their actions."[197] Deliberately boosting ambiguity may prove effective against most adversaries, but it seems counterproductive when trying to deter an assertive China. Thus, US military commanders, their staffs, and policymakers require an appreciation for the nuances of China's views on cyber operations. As a sophisticated actor in cyberspace, China warrants a sophisticated cyber defense policy that appreciates its particularities.

Today, doctrinal confusion in the cyber domain appears untenable. The US-supported multi-stakeholder approach to Internet governance has failed to persuade many governments that seem apt to support Beijing and Moscow. If an open Internet is a US strategic interest, the erosion of multi-stakeholder governance should alarm strategists. In today's information environment, China continues to pursue cyber sovereignty, which fundamentally clashes with America's vision. As these two great powers pursue incompatible strategic objectives in cyberspace, their ambitions seem ripe for confrontation. To prevent such disputes from accidently spiraling out of control, Beijing and Washington must clarify their doctrinal differences and develop mechanism for de-escalation to avoid the calamity of a cyber war.

NOTES

1. “Chinese military launches two new wings for space and cyber age,” *South China Morning Post*, January 1, 2016, accessed January 3, 2016, http://www.scmp.com/news/china/diplomacy-defence/article/1897356/chinese-military-launches-two-new-wings-space-and-cyber.

2. “China: The Power of Military Organization,” *Stratfor,* January 25, 2016, accessed March 12, 2016, https://www.stratfor.com/analysis/china-power-military-organization.

3. David M. Finkelstein, “Initial Thoughts on the Reorganization and Reform of the PLA,” *CNA Occasional Paper* (January 15, 2016), 2.

4. Zhang Jianfeng, ed., “China inaugurates PLA Rocket Force as military reform deepens,” *Xinhua*, January 2, 2016.

5. John Costello, “The Strategic Support Force: China’s Information Warfare Service,” *China Brief* 16, No. 3 (February 8, 2016), accessed March 12, 2016, http://www.jamestown.org/single/?tx_ttnews%5Btt_news%5D=45075&no_cache=1#.VubSypMrJE4.

6. “Expert: PLA Strategic Support Force a key force to win wars,” *China Military Online*, January 6, 2016, accessed January 7, 2016, http://eng.mod.gov.cn/TopNews/2016-01/06/content_4635472.htm.

7. Wu Gang, “China upgrades missile force, adds space and cyber war forces,” *Global Times*, January 1, 2016, accessed January 9, 2016, http://www.globaltimes.cn/content/961440.shtml.

8. Mark A. Stokes, Jenny Lin and L.C. Russell Hsiao, “The Chinese People’s Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure,” *Project 2049 Institute* (November 11, 2011), 7.

9. Lü Jinghua [吕晶华], “Gongtong goujian heping anquan kaifang hezuo de wangluo kongjian,” [共同构建和平安全开放合作的网络空间] (Jointly building a peaceful and safe cyberspace through open cooperation) *PLA Daily,* October 18, 2016, http://www.81.cn/jfjbmap/content/2015-10/18/content_126334.htm.

10. Stuart N. Brotman, “Multistakeholder Internet governance: A pathway completed, the road ahead,” *Brookings Institution* (July 2015), 6, accessed March 18, 2016, http://www.brookings.edu/~/media/research/files/papers/2015/07/20-multistakeholder-internet-governance-brotman/multistakeholder.pdf.

11. Evan Osnos, A*ge of Ambition: Chasing Fortune, Truth, and Faith in the New China,* Farrar, Straus and Giroux. Kindle Edition, 95.

12. Li Xiguang and Wang Jing, “The Role of E-diplomacy in Iranian and Xinjiang Riots,” in *Media, Powerm and Politics in the Digital Age* edited by Yahya R. Kamalipour (Lanham, MD: Rowman and Littlefield Publishers, 2010), 148.

13. Jing Li, “China blocks VPN services that let users get round its ‘Great Firewall’ during big political gatherings in Beijing,” *South China Morning Post,* March 9, 2016, accessed March 21, 2016, http://www.scmp.com/news/china/policies-politics/article/1922677/china-blocks-vpn-services-let-users-get-round-its-great.

14. Ibid.

15. Elsa Kania, “China's Military Strategy: A Cyber Perspective,” *Real Clear Defense,* June 3, 2015, accessed January 5, 2015, http://www.realcleardefense.com/articles/2015/06/03/chinas_military_strategy_a_cyber_perspective_108008.html.

16. Lu Wei (鲁炜), “Jianchi zunzhong wangluo zhuquan yuance tuidong goujian wangluo kongjian mingyun gongtongti” [坚持尊重网络主权原则 推动构建网络空间命运共同体] (Adhere on respect for the principle of cyber sovereignty to promote and build cyberspace community of destiny), *Quishi,* February 29, 2016, accessed March 18, 2016, http://www.qstheory.cn/dukan/qs/2016-02/29/c_1118164592.htm.

17. Li Minghai [李明海], “Dazao quanxin de wangluo ‘zuozhan liliang’,” [李明海：打造全新的网络“作战力量”] (Li Minghai: Forging a new network of ‘Combat Power’), *Morning Post,* accessed March 18, 2016, http://www.morningpost.com.cn/2016/0121/1246606.shtml.

18. John Palfrey, “The end of the experiment: How ICANN's foray into global internet democracy failed,” *Harvard Journal of Law & Technology* 17, No. 2 (2004), 412.

19. “Five Key Takeaways from ICANN 55,” *Mayer Brown Legal Update* (April 25, 2016), 1.

20. Palfrey, “The end of the experiment: How ICANN's foray into global internet democracy failed,” 420.

21. Amar Toor, “Will the global NSA backlash break the internet?” November 8, 2013, accessed May 14, 2016, http://www.theverge.com/2013/11/8/5080554/nsa-backlash-brazil-germany-raises-fears-of-internet-balkanization.

22. Gui Tao, “China Voice: Time to reconsider Internet freedom touted by U.S.,” *Xinhua,* December 15, 2015, accessed March 21, 2016, http://news.xinhuanet.com/english/2015-12/15/c_134918998.htm.

NOTES

23. Zachary Keck, "Has Snowden Killed Internet Freedom?" *The Diplomat,* July 13, 2013, accessed May 13, 2016, http://thediplomat.com/2013/07/has-snowden-killed-internet-freedom/.

24. Hogan Lovells, "ICANN sets course for change of Internet stewardship," *LimeGreen IP* (April 7, 2016), accessed May 12, 2016, http://www.lexology.com/library/detail.aspx?g=b8f5da45-7169-4e39-9834-f84b9f318518.

25. Ibid., 3.

26. Stephen Karmazyn, "Deadline looms for U.S. to cede control over Internet naming conventions," *Globe and Mail,* May 8, 2016, accessed May 12, 2016, http://www.theglobeandmail.com/technology/deadline-looms-for-us-to-cede-control-over-internet-naming-conventions/article29933641/.

27. *Wuzhen Report on World Internet Development 2016* (November 18, 2016), accessed December 20, 2016, http://www.wuzhenwic.org/2016-11/18/c_61834.htm.

28. "China Cyber: Stepping Into the Shoes of a 'Major Power'," *EastWest Institute* (December 5, 2016), accessed December 20, 2016, https://www.eastwest.ngo/idea/china-cyber-stepping-shoes-"major-power"

29. Li Minghai, "Forging a new network of 'Combat Power'."

30. Bill Gertz, "PLA on cyberwarfare buildup," *Washington Times,* February 17, 2016, accessed March 20, 2016, http://www.washingtontimes.com/news/2016/feb/17/inside-the-ring-china-plans-cyberwarfare-force-to-/?page=all.

31. "Lun xinshiji xinjieduan wo jun de lishi shiming," [论新世纪新阶段我军的历史使命], *PLA Daily,* June 19, 2007, accessed March 9, 2016, http://news.xinhuanet.com/zgjx/2007-06/19/content_6262236.htm.

32. "Possible Push to Elevate US Cyber Command in Fight vs IS," *Voice of America,* April 5, 2016, accessed April 6, 2016, http://www.voanews.com/content/possible-push-elevate-us-cyber-command-fight-islamic-state/3270815.html.

33. Greg Masters, "Senate sends bill to Obama to elevate Cyber Command," *SC Media* (December 12, 2016), accessed December 19, 2016, https://www.scmagazine.com/senate-sends-bill-to-obama-to-elevate-cyber-command/article/578482/.

34. Laura Galante, "What To Watch: U.S.-China Cyber Talks Commence" *FireEye Blog* (December 11, 2015), accessed February 4, 2015, https://www.fireeye.com/blog/executive-perspective/2015/12/what_to_watch_u_s-.html.

35. Everett Rosenfeld, "US-China agree to not conduct cybertheft of intellectual property," *Reuters,* September 25, 2015.

36. Corey Bennett, "Obama talks cyber with Chinese President Xi Jinping," *The Hill,* March 31, 2016, accessed April 9, 2016, http://thehill.com/policy/cybersecurity/274845-obama-talks-cyber-with-chinese-president-xi-jinping.

37. "Third U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues," *Department Homeland Security* (December 7, 2016), accessed December 20, 2016, https://www.dhs.gov/news/2016/12/08/third-us-china-high-level-joint-dialogue-cybercrime-and-related-issues.

38. 2006 *Quadrennial Defense Review* (Washington, DC: US Department of Defense, February 6, 2006), 29.

39. 2014 *Quadrennial Defense Review* (Washington, DC: US Department of Defense, March 4, 2014), 7.

40. Franklin D. Kramer, Stuart H. Starr, Larry Wentz, *Cyberpower and National Security* (Kindle Edition: Potomac Books, 2009), 47.

41. Joint Publication (JP) 3-12(R) *Cyberspace Operations* (Washington, DC: Joint Staff, February 5, 2013), I-2.

42. David Raymond, Tom Cross, Gregory Conti and Michael Nowatkowski, "Key Terrain in Cyberspace: Seeking the High Ground," in *6th International Conference on Cyber Conflict* edited by P.Brangetto, M. Maybaum and J. Stinissen (Tallinn, Estonia: NATO CCD COE Publications, 2014): 298; Bryan Krekel, Patton Adams and George Bakos, "Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage" (Report prepared for US-China Economic and Security Review Commission by Northrop Grumman Corp, Washington DC, March 7, 2012), 299.

43. David K. Edmonds, "In Search of High Ground: The Airpower Trinity and the Decisive Potential of Airpower," *Airpower Journal* (Spring 1998), accessed April 6, 2016, http://www.airpower.maxwell.af.mil/airchronicles/apj/apj98/spr98/edmonds.html.

44. Ye Zheng, "Dui wangluo zhuquan de sikao," *Renmin Wanglilun* pindao, July 20, 2015, accessed January 9, 2016, http://theory.people.com.cn/n/2015/0720/c386965-27332547.html.

NOTES

45. An Weiping, “Deputy army commander: China should develop trump card forces,” *China Military Online,* January 15, 2016, accessed March 22, 2016, http://english.chinamil.com.cn/news-channels/pla-daily-commentary/2016-01/15/content_6858982.htm.

46. Ibid.

47. Zhu Ningning, “Jiefangjun fujunzhang: jundui ying youxiao wangluo fankong renwu,” [解放军副军长：军队应有效履行网络反恐任务] (Deputy Commander of the PLA: The PLA should carry out effective counterterrorism mission in cyberspace) *PLA Daily,* January 7, 2016, accessed March 22, 2016, http://www.chinanews.com/m/mil/2016/01-07/7705750.shtml.

48. An Weiping, “Deputy army commander: China should develop trump card forces”.

49. Graham T. Allison and Morton H. Halperin, “Bureaucratic Politics: A Paradigm and Some Policy Implications,” *World Politics* 24, Supplement: Theory and Policy in International Relations (Spring 1972), 53.

50. Jerel A. Rosati, “Developing a Systematic Decision-Making Framework: Bureaucratic Politics in Perspective,” *World Politics* 33, No. 2 (January 1981), 236.

51. Jason Healey, “Comparing Norms for National Conduct in Cyberspace,” *New Atlanticist,* June 20, 2011, accessed January 9, 2016, http://www.atlanticcouncil.org/about/experts/list/jason-healey.

52. Internet Governance Progress After ICANN 53: Hearing Before Subcommittee on Communications and Technology Committee on Energy and Commerce United States House of Representatives, 114th Cong. (July 8, 2015) (Lawrence E. Strickling, Assistant Secretary for Communications and Information, National Telecommunications and Information Administration, US Department of Commerce, Washington DC).

53. Nicholas Dynon, “The Future of Cyber Conflict: Beijing Rewrites Internet Sovereignty Along Territorial Lines,” *Jamestown Foundation China Brief* 15, No. 17 (September 4, 2015), accessed January 10, 2016, http://www.jamestown.org/programs/chinabrief/single/?tx_ttnews%5Btt_news%5D=44338&cHash=1622a6ba07e8dfa6844d135dfaf073ad#.VpUI0pMrJE4.

54. Adam Segal, “China’s Internet Conference: Xi Jinping’s Message to Washington,” *Council on Foreign Relations,* December 16, 2015, http://blogs.cfr.org/cyber/2015/12/16/chinas-internet-conference-xi-jinpings-message-to-washington/.

55. Stuart N. Brotman, “Multistakeholder Internet governance: A pathway completed, the road ahead,” *Brookings Institution* (July 2015), 6, accessed March 18, 2016, http://www.brookings.edu/~/media/research/files/papers/2015/07/20-multistakeholder-internet-governance-brotman/multistakeholder.pdf.

56. Huaxia, ed., “Highlights of Xi's Internet speech,” *Xinhua,* December 16, 2015, accessed January 11, 2016, http://news.xinhuanet.com/english/2015-12/16/c_134923855.htm.

57. Ibid.

58. Ye Zheng, “From Cyberwarfare to Cybersecurity in the Asia-Pacific and Beyond,” translated by Yang Fan in *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain,* edited by Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron (London: Oxford Scholarship Online, April 2015), 132, doi:10.1093/acprof:oso/9780190201265.001.0001.

59. Ye Zheng, “Dui wangluo zhuquan de sikao,” *Renmin Wanglilun pindao,* July 20, 2015, accessed January 9, 2016, http://theory.people.com.cn/n/2015/0720/c386965-27332547.html.

60. Scott D. Livingston, “Beijing Touts ‘Cyber-Sovereignty’ In Internet Governance: Global Technology Firms Could Mine Silver Lining,” *ChinaFile* (February 19, 2015), accessed January 10, 2016, https://www.chinafile.com/reporting-opinion/viewpoint/beijing-touts-cyber-sovereignty-internet-governance.

61. *DoD Cyber Strategy* (Washington DC: Office of the Secretary of Defense, April 2015), 1.

62. *People's Republic of China Cybersecurity Law* (Draft), National People’s Congress, accessed March 23, 2016, http://www.npc.gov.cn/npc/xinwen/lfgz/flca/2015-07/06/content_1940614.htm.

63. *Zhongguo de junshi zhanlüe* (Beijing: State Council Information Office of the People's Republic of China, May 2015), accessed January 8, 2016, http://www.scio.gov.cn/zfbps/gfbps/Document/1435341/1435341.htm.

64. “Xi pledges ‘great renewal of Chinese nation’” *Xinhua,* November 29, 2012, accessed January 10, 2016, http://news.xinhuanet.com/english/china/2012-11/29/c_132008231.htm.

65. “Full Transcript: Interview With Chinese President Xi Jinping,” *Wall Street Journal,* September 22, 2015, accessed January 10, 2016, http://www.wsj.com/articles/full-transcript-interview-with-chinese-president-xi-jinping-1442894700.

NOTES

66. "Chapter IV: Building and Development of China's Armed Forces," *China's Military Strategy* (May 26, 2015), accessed March 22, 2016, http://news.xinhuanet.com/english/china/2015-05/26/c_134271001_4.htm.

67. Luo Zheng [罗铮] "Junshi zhuanjia jiedu xinban guofang baipishu," [军事专家解读新版国防白皮书] (Military expert interpret the new defense white paper), *PLA Daily,* May 26, 2015, accessed March 22, 2016, http://jz.chinamil.com.cn/gd/2015-05/26/content_6507585.htm.

68. Song Xiaojun, "Zhongguo Xinban guofan baipishu 30 nianlai zui xiangxi," *Fenghuang xin meiti* (May 26, 2015), accessed January 14, 2016, http://v.ifeng.com/mil/mainland/201505/012b32da-beb1-4a9b-9d30-38d87c592420.shtml.

69. Yang Yucai, "White paper states China's peaceful intention," *Global Times,* May 5, 2015, accessed January 10, 2016, http://www.globaltimes.cn/content/924594.shtml.

70. Anthony H. Cordesman and Steven Colley, "Chinese Strategy and Military Modernization in 2015: A Comparative Analysis," *Center for Strategic and International Studies* (October 10, 2015), 121.

71. Toshi Yoshihara and James Holmes, Red Star over the Pacific: *China's rise and the challenge to US maritime strategy* (Annapolis, MD: Naval Institute Press, 2011), x.

72. Alison A. Kaufman and Daniel M. Hartnett, "Managing Conflict: Examining recent PLA writings on escalation control," CNA (February 2016), 5.

73. Luo Zheng, "Military expert interpret the new defense white paper."

74. Song Puxuan [宋普选], "Beibu zhanqu siling yuan: Jiajin qianghua suishi dahang huangtai" [北部战区司令员：加紧强化随时打仗状态] (Northern Military Region Commander: Intensifying and strengthening responsiveness for contingencies), *PLA Online,* March 15, 2016, accessed March 22, 2016, http://www.chinanews.com/mil/2016/03-15/7797840.shtml.

75. Huang Xiang [黄集骧], deputy director of political work for the Western Region, "Jujiao "zhuzhan" tuidong zhengzhi jiguan zhuanxing" [聚焦"主战"推动政治机关转型] (Focus on the "battle" to promote political reorganization), *PLA Online,* March 16, 2016, accessed March 22, 2016, http://www.81.cn/jfjbmap/content/2016-03/16/content_137936.htm.

76. Ben Lowsen, "How China Fights: The PLA's Strategic Doctrine," *The Diplomat,* April 6, 2016, accessed April 7, 2016, http://thediplomat.com/2016/04/how-china-fights-the-plas-strategic-doctrine/.

77. Alison A. Kaufman and Daniel M. Hartnett, "Managing Conflict: Examining recent PLA writings on escalation control," 1.

78. M. Taylor Fravel, "The evolution of china's military strategy: comparing the 1987 and 1999 editions of zhanlüexue," in *China's Revolution in Doctrinal Affairs: Emerging Trends in the Operational Art of the Chinese People's Liberation Army,* edited by James Mulvenon and David M. Finkelstein (Alexandria, Virginia: CNA, December 2005), 85.

79. Luo Zheng, "Military expert interpret the new defense white paper."

80. *China's Military Strategy* (US Naval Institute, May 26, 2015), accessed January 9, 2016, http://news.usni.org/2015/05/26/document-chinas-military-strategy.

81. David M. Finkelstein, "China's National Military Strategy," in *The People's Liberation Army in the Information Age* by James C. Mulvenon and Richard H. Yang, eds., (Santa Monica, CA: RAND Corporation, 1999), 103.

82. Ibid.

83. Derek S. Reveron and James L. Cook, "Developing strategists: Translating National Strategy into Theater Strategy," *Joint Forces Quarterly* 55 (4th Quarter 2009): 24.

84. Derek S. Reveron and James L. Cook, "Developing strategists: Translating National Strategy into Theater Strategy," 23.

85. Lin Dong [林东], "Guanyu zhanlüe xue chuangxin fazhan de sikao" [关于战略学创新发展的思考] (On the Innovative Development of the Science of Strategy), *Junshi Kexue* (April 1, 2014): 79.

86. Song Puxuan, "Northern Military Region Commander: Intensifying and strengthening responsiveness for contingencies".

87. Michael D. Swaine, "Xi Jinping's Address to the Central Conference on Work Relating to Foreign Affairs: Assessing and Advancing Major- Power Diplomacy with Chinese Characteristics," *China Leadership Monitor* 46 (March 19, 2015), 11, accessed January 10, 2016, http://www.hoover.org/research/xi-jinpings-address-central-conference-work-relating-foreign-affairs-assessing-and.

NOTES

88. Robert Lawrence Kuhn, “Xi Jinping’s Chinese Dream,” *New York Times,* June 4, 2013.

89. An, “Growing China to contribute more to Asia development: Xi,” *Xinhua,* October 29, 2014, http://news.xinhuanet.com/english/china/2014-10/29/c_133752083.htm.

90. Yin Pumin, “Mapping Out Success: New five-year blueprint lays down specific objectives for a prosperous China,” *Beijing Review* 45 (November 5, 2015), accessed January 10, 2016, http://www.bjreview.com.cn/Current_Issue/Editor_Choice/201511/t20151102_800041696.html.

91. Xi Jinping, “Working Together to Forge a New Partnership of Win-win Cooperation and Create a Community of Shared Future for Mankind,” Speech, United Nations, New York, NY, September 22, 2015, accessed January 10, 2016, http://qz.com/512886/read-the-full-text-of-xi-jinpings-first-un-address/.

92. Michael D. Swaine, “Xi Jinping’s Address to the Central Conference on Work Relating to Foreign Affairs: Assessing and Advancing Major- Power Diplomacy with Chinese Characteristics.”; Xi Jinping, “Chinese President Xi Jinping Addresses the American Public,” Speech, National Committee on U.S.-China Relations, Seattle, WA, September 22, 2015, accessed January 10, 2016, https://www.ncuscr.org/content/full-text-president-xi-jinpings-speech.

93. Wang Hongguang [王洪光], “Wang Hongguang tan lianghui: Bushi dongbeiya shengwen wei zhuyao zhanlüe fangxiang” [王洪光谈两会：不使东北亚升温为主要战略方向] (Northeast Asia is not the strategic direction that is heating up), *Sohu,* March 2, 2016, accessed March 19, 2016, http://mil.sohu.com/20160302/n439166845.shtml.

94. Ibid.

95. Wang Hongguang, “Lt. Gen. Wang Hongguang: no such thing as "giving up DPRK" for China,” *China Military Online,* December 2, 2014, accessed March 18, 2016, http://english.chinamil.com.cn/news-channels/china-military-news/2014-12/02/content_6251361.htm.

96. Yao Runping, ed., “President Hu Jintao asks officials to better cope with Internet,” *Xinhua,* January 24, 2007, accessed January 10, 2016, http://news.xinhuanet.com/english/2007-01/24/content_5648674.htm.

97. Wang Xixin [王西欣], “Zai lun kongzhizhan,” [再论控制战] (Further discussion on war of control), *Junshi Kexue* (April 15, 2014), 66.

98. International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World (Washington DC: The Office of the President, May 2011), 5.

99. Adam Segal, “Chinese responses to the International Strategy for Cyberspace,” *Council for Foreign Relations* (May 23, 2011), accessed January 9, 2016, http://blogs.cfr.org/asia/2011/05/23/chinese-responses-to-the-international-strategy-for-cyberspace/.

100. Ye Zheng and Zhao Baoxian, “Wangluo zhan, zenme zhan?” *Zhongguo Qingnian bao,* June 3, 2011, accessed January 9, 2016, http://zqb.cyol.com/html/2011-06/03/nw.D110000zgqnb_20110603_1-09.htm.

101. *China’s Military Strategy* (US Naval Institute, May 26, 2015), accessed January 9, 2016, http://news.usni.org/2015/05/26/document-chinas-military-strategy.

102. Ibid.

103. *Zhongguo de junshi zhanlüe* (Beijing: State Council Information Office of the People's Republic of China, May 2015), accessed January 8, 2016, http://www.scio.gov.cn/zfbps/gfbps/Document/1435341/1435341.htm.

104. Luo Zheng, “Military expert interpret the new defense white paper”.

105. Franklin D. Kramer, Stuart H. Starr, Larry Wentz, *Cyberpower and National Security* (Kindle Edition: Potomac Books, 2009), 37.

106. Ibid.

107. 2006 *Quadrennial Defense Review,* 32.

108. US Cyber Deterrence Strategy (Washington DC: the White House, December 18, 2015), 3, accessed March 22, 2016, http://fedscoop.com/obama-cybersecurity-deterrence-strategy.

109. Michael Johnson and Terrence K. Kelly, “Tailored Deterrence: Strategic Context to Guide Joint Force 2020,” *Joint Forces Quarterly* 74 (3rd Quarter 2014): 26.

110. Rhea Siers, “The Myth of Cyber Deterrence,” *The Cipher Brief* (March 3, 2016), accessed March 22, 2016, https://www.thecipherbrief.com/article/techcyber/myth-cyber-deterrence.

NOTES

111. Peter Singer, "How the United States Can Win the Cyberwar of the Future: Cold War-era deterrence theory won't cut it anymore," *Foreign Policy,* December 18, 2015, accessed March 22, 2016, http://foreignpolicy.com/2015/12/18/how-the-united-states-can-win-the-cyberwar-of-the-future-deterrence-theory-security/.

112. Ibid.

113. Graham Webster, "America Can't Deter What It Can't Define in Cyberspace," *The Diplomat,* August 13, 2015, accessed March 22, 2016, http://thediplomat.com/2015/08/america-cant-deter-what-it-cant-define-in-cyberspace/.

114. Sarah Weiner, "Searching for Cyber-Deterrence," *Center for Strategic and International Studies* (November 26, 2012), accessed March 22, 2016, http://csis.org/blog/searching-cyber-deterrence/.

115. US *Cyber Deterrence Strategy.*

116. Lisa O. Monaco, "Administration Efforts on Cybersecurity: The Year in Review and Looking Forward to 2016," *White House* (February 2, 2016), accessed March 22, 2016, https://www.whitehouse.gov/blog/2016/02/02/administration-efforts-cybersecurity-year-review-and-looking-forward-2016.

117. Ibid.

118. Andrew Blake, "John McCain says White House's cyber deterrence policy comes up short," *Washington Times,* January 15, 2016, accessed March 22, 2016, http://www.washingtontimes.com/news/2016/jan/15/john-mccain-says-white-houses-cyber-deterrence-pol/.

119. Katie Bo Williams, "McCain blasts White House cyber policy," *The Hill,* January 15, 2016, accessed March 18, 2016, http://thehill.com/policy/cybersecurity/266104-mccain-blasts-white-house-cyber-policy.

120. Joint Publication (JP) 1-02 *Department of Defense Dictionary of Military and Associated Terms* (Washington, DC: Joint Staff, February 15, 2016), 67.

121. Kevin Pollpeter, "Chinese Writings on Cyber Warfare and Coercion," in *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain,* edited by Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron (London: Oxford University Press, March 6, 2015), 147.

122. Rob de Wijk, *The Art of Military Coercion* (Amsterdam, NL: Amsterdam University Press, 2015), 17.

123. Thomas C. Schelling, Arms and Influence (Hartford, CT, USA: Yale University Press, 2008), 71-72.

124. Mingda Qiu, "China's Science of Military Strategy: *Cross-Domain Concepts in the 2013 Edition," Cross-Domain Deterrence (CCD) Working Paper UC San Diego* (September 2015): 10.

125. Dennis J. Blasko, *The Chinese Army Today: Tradition and Transformation for the 21st Century* (New York, NY: Routledge, 2012), 231.

126. Alison A. Kaufman and Daniel M. Hartnett, "Managing Conflict: Examining recent PLA writings on escalation control," 53.

127. Larry M. Wortzel, *The Dragon Extends its Reach* (Kindle Edition: Potomac Books, 2013), Kindle Locations 1550-1551.

128. Dean Cheng, "Prospects for Extended Deterrence in Space and Cyber: The Case of the PRC" (Lecture delivered at the Heritage Foundation, Washington DC, January 21, 2016), 2.

129. Kevin Pollpeter, "Chinese Writings on Cyber Warfare and Coercion."

130. Yuan Yi [袁艺], "Qian xi wangluo kongjian weishe de teheng, leixing he yunyong yaodian," [浅析网络空间威慑的特征、类型和运用要点] (The characteristics, types, and applications of cyberspace deterrence), *People's Daily,* January 4, 2016, accessed March 19, 2016, http://theory.people.com.cn/nl/2016/0104/c386965-28010082.html.

131. Ibid.

132. Yuan Yi, "The characteristics, types, and applications of cyberspace deterrence."

133. Bill Gertz, "Cyber 'People's War' On U.S.," *Washington Times,* June 4, 2014, accessed May 12, 2016, http://m.washingtontimes.com/news/2014/jun/4/inside-the-ring-hagel-to-testify-before-house-pane/.

134. Adam Segal, "From China, an Expansive and Dangerous View of Cyber Deterrence," *Defense One* (January 26, 2016), accessed March 22, 2016, http://www.defenseone.com/threats/2016/01/china-expansive-and-dangerous-view-cyber-deterrence/125418/.

135. Ibid.

NOTES

136. Joseph Marks, “U.S. may punish Chinese hacking before Xi's visit,” September 4, 2015, *Politico,* accessed March 23, 2016, http://www.politico.com/story/2015/09/white-house-chinese-cyber-sanctions-xi-jinping-visit-213360.

137. Erin Kelly, “OPM's cybersecurity chief resigns in wake of massive data breach,” USA *Today,* February 22, 2016, accessed March 23, 2016, http://www.usatoday.com/story/news/2016/02/22/opms-cybersecurity-chief-resigns-amid-continuing-pressure-congress/80766320/.

138. Evan Perez, “U.S. pulls spies from China after hack,” *CNN,* September 3, 2015, accessed March 23, 2016, http://money.cnn.com/2015/09/30/technology/china-opm-hack-us-spies/.

139. Jonathan Chew, “China Says It Wasn't Behind the Massive U.S. Government Hack,” *Fortune,* December 2, 2015, accessed March 23, 2016, http://fortune.com/2015/12/02/china-opm-hack/.

140. Ellen Nakashima, “Chinese government has arrested hackers it says breached OPM database,” *Washington Post,* December 2, 2015, accessed March 23, 2016, https://www.washingtonpost.com/world/national-security/chinese-government-has-arrested-hackers-suspected-of-breaching-opm-database/2015/12/02/0295b918-990c-11e5-8917-653b65c809eb_story.html.

141. Aliya Sternstein, “NSA director: expect more hacks as big as the OPM heist,” *Nextgov,* January 22, 2016, accessed March 23, 2016, http://www.nextgov.com/cybersecurity/2016/01/nsa-director-expect-more-hacks-big-opm-heist/125320/.

142. Colin Clark, “DNI Clapper IDs China As ‘The Leading Suspect’ In OPM Hacks; Russia ‘More Subtle’,” *Breaking Defense,* June 25, 2015, accessed March 23, 2016, http://breakingdefense.com/2015/06/clapper-ids-china-as-the-leading-suspect-in-opm-hacks-russia-more-subtle/.

143. Damian Paletta, “Former CIA Chief Says Government Data Breach Could Help China Recruit Spies,” *Wall Street Journal,* June 15, 2015, accessed March 23, 2016, http://www.wsj.com/articles/former-cia-chief-says-government-data-breach-could-help-china-recruit-spies-1434416996.

144. Julie Hirschfeld Davis and David E. Sanger, “Obama and Xi Jinping of China Agree to Steps on Cybertheft,” *New York Times,* September 25, 2015, accessed March 23, 2016, http://www.nytimes.com/2015/09/26/world/asia/xi-jinping-white-house.html.

145. Adam Segal, “The Top Five Cyber Policy Developments of 2015: United States-China Cyber Agreement,” *Council for Foreign Relations,* January 4, 2016, http://blogs.cfr.org/cyber/2016/01/04/top-5-us-china-cyber-agreement/.

146. Kris Klein, “Cyber Sovereignty: The economic imperatives of a secure cyberspace,” *Prospect: Journal of International Affairs at UCSD* (November 17, 2015), accessed March 23, 2016, http://prospectjournal.org/2015/11/17/cyber-sovereignty-the-economic-imperatives-of-a-secure-cyberspace/.

147. “Chinese President underscores cyber sovereignty, rejects Internet hegemony,” *Xinhua,* December 16, 2014, accessed March 23, 2016, http://news.xinhuanet.com/english/2015-12/16/c_134922689.htm.

148. Jack Goldsmith, “U.S. Attribution of China’s Cyber-Theft Aids Xi’s Centralization and Anti-Corruption Efforts,” *Lawfare* (June 21, 2016), accessed August 15, 2016, https://www.lawfareblog.com/us-attribution-chinas-cyber-theft-aids-xis-centralization-and-anti-corruption-efforts.

149. Ibid.

150. Gregory Kulacki, “The Chinese Military Updates China’s Nuclear Strategy,” *Union of Concerned Scientists* (March 2015), 5, accessed March 18, 2016, http://www.ucsusa.org/sites/default/files/attach/2015/03/chinese-nuclear-strategy-full-report.pdf.

151. Peter Dutton, “Viribus Mari Victoria? Power and Law in the South China Sea” (Paper submitted for “Managing Tensions in the South China Sea” conference, Center for Strategic and International Studies, June 5-6, 2013), 6.

152. Ibid.

153. Ibid.

154. Jon R. Lindsay, “The Impact of China on Cybersecurity: Fiction and Friction,” *International Security 39,* No. 3 (Winter 2014/15): 7-47, doi: 10.1162/ISEC_a_00189.

155. Jon R. Lindsay, “Exaggerating the Chinese Cyber threat,” *Policy Brief, Belfer Center for Science and International Affairs, Harvard Kennedy School* (May 2015), accessed March 12, 2015, http://belfercenter.ksg.harvard.edu/files/linsday-china-cyber-pb-final.pdf.

NOTES

156. Jon R. Lindsay, "The Impact of China on Cybersecurity: Fiction and Friction."

157. Twomey, *The Military Lens: Doctrinal Difference and Deterrence Failure in Sino-American Relations,* 4.

158. Allen Suess Whiting, China crosses the Yalu: *The decision to enter the Korean War* (Stanford University Press, 1968), 156.

159. Richard W. Stewart, "The Chinese Intervention," in *The Korean War* (US Army Center of Military History, March 8, 2002), 33.

160. National Security Council Report, NSC 81/1, "United States Courses of Action with Respect to Korea," September 9, 1950, accessed March 12, 2016, http://digitalarchive.wilsoncenter.org/document/116194.

161. Twomey, *The Military Lens: Doctrinal Difference and Deterrence Failure in Sino-American Relations,* 94.

162. Ibid, 106.

163. Ibid, 111.

164. Ibid, 121.

165. Ibid, 132.

166. Ibid.

167. Ibid.

168. "Korean War Fast Facts," CNN, July 3, 2015, accessed March 23, 2016, http://www.cnn.com/2013/06/28/world/asia/korean-war-fast-facts/.

169. David Shambaugh, "PLA Strategy & Doctrine: Recommendations for a Future Research Agenda" (Discussion paper prepared for "Chinese Military Studies: a Conference on the State of the Field" at the US National Defense University Institute for National Strategic Studies' Center for the Study of Chinese Military Affairs, Fort McNair, Virginia, October 26-27, 2000), accessed March 12, 2016, http://www.comw.org/cmp/fulltext/0010shambaugh.htm.

170. Cheng Jun (程军), "Huayang diechu de meijunjunshi lilun: Jiduo shi tansuo jiduo shi huyou" [Persistent patterns of US military doctrine: How much is exploration? How much is manipulation?] *PLA Daily,* October 14, 2010, accessed March 16, 2016, http://theory.people.com.cn/GB/12954938.html.

171. Joint Chiefs of Staff J7, "The Role of Multinational Joint Doctrine," *Joint Forces Quarterly,* no. 67 (4th Quarter, 2012), 111.

172. Alison A. Kaufman and Peter W. Mackenzie, "Field Guide: The Culture of the Chinese People's Liberation Army," 25.

173. Christopher P. Twomey, *The Military Lens: Doctrinal Difference and Deterrence Failure in Sino-American Relations* (Ithaca, NY: Cornell University Press, 2010), 243.

174. Twomey, *The Military Lens: Doctrinal Difference and Deterrence Failure in Sino-American Relations,* 243.

175. Graham Webster, "America Can't Deter What It Can't Define in Cyberspace," *The Diplomat,* August 13, 2015, accessed March 22, 2016, http://thediplomat.com/2015/08/america-cant-deter-what-it-cant-define-in-cyberspace/.

176. 2015 *National Military Strategy* (Washington DC: Joint Staff, June 2015), 4.

177. Ibid.

178. Ibid.

179. TRADOC Pamphlet 525-3-1 *US Army Operating Concept: Winning in a Complex World 2020-2040* (Washington, DC: Army Staff, October 31, 2014), 7.

180. Ibid, 16.

181. Wang Xixin [王西欣], "Zai lun kongzhizhan," [再论控制战] (Further discussion on war of control), *Junshi Kexue* (April 15, 2014), 64.

182. Alison A. Kaufman and Daniel M. Hartnett, "Managing Conflict: Examining recent PLA writings on escalation control," *CNA* (February 2016), 1.

183. Lin Dong [林东], "Guanyu zhanlüe xue chuangxin fazhan de sikao" [关于战略学创新发展的思考] (On the Innovative Development of the Science of Strategy), *Junshi Kexue* (1 April 2014), 79.

184. Adam Segal, "Stabilizing Cybersecurity in the U.S.-China Relationship," *Council for Foreign Relations* (September 14, 2015), accessed March 12, 2016, http://nbr.org/research/activity.aspx?id=605.

185. Ibid.

NOTES

186. General Assembly resolution 64/211, Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures, A/RES/64/211/Add 3 (December 21, 2009).

187. Cheryl Pellerin, "U.S., China Must Work Together on Cyber, Panetta Says," *American Forces Press Service – DoD News,* May 7, 2012, accessed March 12, 2016, http://archive.defense.gov/news/newsarticle.aspx?id=116235.

188. Michele Markoff, "Developments of Cyberspace and Emerging Challenges" (Remarks for panel session at ARF Workshop on cyber capacity building, Beijing, China, July 28, 2015), accessed March 12, 2016, http://beijing.usembassy-china.org.cn/mobile/2015/arf-workshop-on-cyber-capacity-building.html.

189. "U.S.-China Strategic and Economic Dialogue Outcomes of the Strategic Track," *US Department of State* (July 14, 2014), accessed March 13, 2016, http://www.state.gov/r/pa/prs/ps/2014/07/229239.htm.

190. Xu Lin, "Zhongmei duihua you zhu zengxinshiyi," [US-China Dialogue will help enhance mutual trust] *PLA Daily,* July 10, 2014, accessed March 13, 2016, http://navy.81.cn/content/2014-07/10/content_6041990.htm.

191. Takeshi Yamawaki, "Interview/ Kurt Campbell: China should think carefully about provoking South China Sea tensions," *Ashi Shimbun,* June 20, 2015, accessed January 15, 2016, http://ajw.asahi.com/article/views/opinion/AJ201506200060.

192. Kimberly Field and Stephan Pikner, "The Role of U.S. Land Forces in the Asia-Pacific," *Joint Forces Quarterly* 74 (3rd Quarter 2014), 33.

193. Ibid.

194. Remarks by President Obama and President Xi of the People's Republic of China in Joint Press Conference, Washington DC, September 25, 2015, accessed March 12, 2016, https://www.whitehouse.gov/the-press-office/2015/09/25/remarks-president-obama-and-president-xi-peoples-republic-china-joint.

195. "Xinjinping chuxi baigong huanying yishi aobama zhongwen shuo 'ni hao' zhiyi," [习近平出席白宫欢迎仪式 奥巴马中文说"你好"致意], *China National Radio,* September 26, 2015, accessed March 13, 2016, http://china.cnr.cn/yaowen/20150926/t20150926_519982837.shtml.

196. Graham Webster, "Has U.S. Cyber Pressure Worked on China? Read those leaks carefully," *The Diplomat,* December 10, 2015, accessed March 13, 2016, http://thediplomat.com/2015/12/has-u-s-cyber-pressure-worked-on-china/.

197. *US Cyber Deterrence Strategy,* 5.