The Art of (Cyber) War

Brian M. Mazanec

The People's Republic of China (PRC) is increasingly developing and fielding advanced capabilities in cyberspace. These capabilities focused not only on collecting sensitive information, but also on achieving military ef capable of causing economic harm, damaging critical infrastructure, and influencing the outcome of conventi armed conflicts.

China, in other words, is interested in cyberwarfare as a t of national power, and is greatly improving its capabilities conduct military operations in cyberspace. In its most recen report to Congress on China's military power, the Pentagon noted that "China's strategic strike capabilities… are expar from the land, air, and sea dimensions of the traditional battlefield into the… cyber-space domains."[1] Understandir China's cyberwarfare strategy will provide valuable insight its future ambitions, principally in light of the U.S.'s heavy reliance on the cyberspace domain from both a military and economic standpoint.

The roots of Chinese cyberwarfare

In many ways, China's contemporary focus on cyberwarfar an extension of traditional Chinese stratagems, namely Su Tzu's "overcoming the superior with the inferior" (i.e., asymmetric warfare) and Chairman Mao Zedong's concept c "People's War." It is intimately connected to the country's

broader geopolitical strategic interests: regime survival; dominance in the Asia/Pacific region; growing influence on global level; and prevention of Taiwan's independence, coup with its ultimate assimilation into the PRC.[2]

Cyberwarfare has been a pillar of Chinese military strateg since the early 1990s, when the Gulf War provided China's leaders with a painfully clear example of the importance of technological superiority and the advantage "informationali forces possess over their less advanced opponents. PRC strategists quickly came to embrace the Revolution in Milit Affairs (RMA) and believed the future of warfare would increasingly rely on denying or degrading an enemy's information flow, rather than simple kinetic firepower. This particularly true when one considers a theoretical Sino-U.S conflict, in which U.S. military power would be difficult if n impossible to defeat head-on. Thus, in their infamous 1999 manifesto, *Unrestricted Warfare*, People's Liberation Army (PLA) Colonels Qiao Liang and Wang Xiangsui proposed a f of warfare that "transcends all boundaries and limits," and exploits the central role that cyberspace plays in future conflict.[3]

A decade on, the results are striking. In recent years, the has steadily leveraged its rapidly growing economy to adva its capabilities to act in cyberspace. As Richard Lawless, th Deputy Undersecretary for Defense for Asian and Pacific Security Affairs, noted back in 2007: "Chinese capabilities i this area have evolved from defending networks from attacl offensive operations against adversary networks… [They ar leveraging information technology expertise available in China's booming economy to make significant strides in cyb warfare."[4]

Summary of nation-state cyberwarfare capabilities

	China	India	Iran	N. Korea	Pakistan	Russia
Official cyber-warfare doctrine	X	X			*Probable*	X
Cyberwarfare training	X	X	X		X	
Cyberwarfare exercises/simu-lations	X	X				
Collaberation with IT industry and/or technical universities	X	X	X		X	X
IT road map	*likely*	X				
Information warfare units	X	X		X		
Record of hack-ing other nations	X					X

Adapted from Charles Billo and Welton Chang, "Cyber Warfare: An Analysis of the Means and Motivations of Selected Nation States," Institute for Security Technology Studies, Dartmouth College, December 2004.

Beijing's notorious lack of transparency regarding its arm forces has made the scope of China's cyberwarfare capabilit difficult to determine. What is clear, however, is that the P is heavily investing in cyberwarfare relative to other natior Equally evident is that their investments are paying major dividends. According to a 2008 study by Dartmouth College Institute for Security Technology Studies, China alone amo other potential U.S. competitors has developed the full spectrum of capabilities and practices for cyberspace domin and cyberwarfare.[5]

China's leaders did not develop this capability overnight. Their interest in cyberwarfare led to a sustained investmen asymmetric disruptive capabilities. As early as 2003, the P had already organized its first cyberwarfare units.[6] Since t these cadres have leveraged China's economy to force IT companies, most significantly Microsoft, to reveal sensitive proprietary information regarding their software and applications.[7] This information allows the PLA to utilize "zero-day" security flaws in Microsoft Office applications th exploit unknown or un-patched software vulnerabilities bef the vendor patch is available.[8] It also greatly enhances the PRC's ability to plant malicious software designed to collec sensitive information or potentially damage networks and infrastructure.

Perhaps the best example of China's burgeoning cyberwar capabilities is known as Titan Rain. The Titan Rain cyber attacks occurred from 2003 to 2005, and involved systemati intrusions into hundreds of U.S. government computers an computer networks of America's Western European allies. T U.S. media reported that the intrusions originated from thr

routers in the PRC's Guangdong province, and unofficial statements from senior U.S. officials leave little doubt that was a highly sophisticated state-sanctioned Computer Netv Exploitation (CNE) attack from the PRC intended to exfiltr huge amounts of sensitive data.[9] While these CNE attacks damaging and pose serious risks for U.S. national security, are less troubling when compared to the looming threat of Chinese Computer Network Attacks (CNA), which seek to r beyond cyber-espionage in order to achieve real-world milit effects in a true cyberwar.

Why China wages cyberwar

China's interest in achieving military effects via cyberwar begins with deterrence. The goal is not to deter other natio from conducting cyberwarfare against the PRC; rather, it is use the threat of cyberwarfare to deter an actor from behavi in a manner that is in opposition to Chinese strategic inter

In the near term, the PRC's primary focus is the question an independent Taiwan. Chinese planners seek to use cyberwarfare to deter U.S. military involvement in a hostile reunification scenario with Taiwan.[10] One advantage of threatening strategic cyberwarfare for a deterrence impact that it is a more realistic threat when compared to the thre other strategic weapons such as nuclear weapons. It is high implausible that the PRC would use its limited *force de fra* to keep the U.S. out of the Formosa Strait, especially in ligh its no-first-use policy.[11] But a strategic cyberwarfare attac with less international stigma and a likely more restrained retaliatory response, is more credible. Furthermore, the challenge of attribution in cyberspace provides China with plausible deniability and makes cyberwarfare all the more attractive. "Independent" patriotic hackers, cultivated and loosely controlled as a 21st-century version of Mao's "People War," provide the perfect mechanism to give the PRC cyber threat credibility.

Deterrence theory has been largely associated with nuclea policy, but its application extends to cyberwarfare. During t Cold War, the U.S. and Soviet Union adopted a survivable nuclear force to present a credible deterrent that maintaine the "uncertainty" inherent in a strategic balance as underst through the accepted theories of Herman Kahn and, later, Thomas Schelling. This arguably prevented a world war through the threat of massive nuclear retaliation—a formul commonly known as Mutually Assured Destruction (MAD).

Deterrence can be both offensive (such as MAD) or defensiv
(deterrence by denial) and based on neutralizing or mitigat
the adversary's undesired action/threat so as to credibly re
the perception that benefits would result from the action.

When one assesses PRC cyberwarfare deterrence, the focu
on the offensive side of the spectrum. For deterrence to
function, the target of deterrence must be a rational actor,
which certainly is the case with the U.S. In fact, the
transparency inherent in U.S. society and government deci
making ensure that its calculus in a conflict such as one
associated with Taiwan would be relatively easy to discern.
only increases the appeal of using cyberwarfare to achieve
successful deterrence. Targets held at risk to achieve deter
are divided into counterforce and countervalue, the former
holding a military target at risk and the latter targeting civ
infrastructure and population or anything else the adversa
values. China believes strategic cyberwarfare is capable of
targeting both of these segments to achieve significant
deterrence effects.

The PRC cyber-threat is not limited to the mere threat of
counterforce/countervalue cyberwarfare to deter an adversa
such as the U.S., however. For the deterrent effects discuss
above to be legitimate and credible, China must actually be
prepared to follow through with the threatened punishmen
action even if deterrence fails. It is likely to do so in respon
one of three principal conflict scenarios.

War over Taiwan

The most likely scenario relates to Taiwan. In the event o
outbreak of hostilities with the island nation, the PLA can
expected to seek a quick knockout blow of Taiwan's defense
while simultaneously delaying U.S. armed forces' entry into
Formosa Strait and then degrading their ability to fight if/o
they have arrived. James Mulvenon, an expert on Chinese
cyberwarfare, has outlined the probable situation as follows

> *For the PLA, using [information warfare] against U.S. information systems to degrade or even delay a deployment of forces to Taiwan offers an attractive asymmetric strategy. American forces are highly information-dependent and rely heavily on precisely coordinated logistics networks… If PLA information operators… were able to hack or*

> *crash these systems, thereby delaying the arrival of a U.S. carrier battle group to the theater, while simultaneously carrying out a coordinated campaign of short-range ballistic missile attacks, "fifth column" and [information warfare] attacks against Taiwanese critical infrastructure, then Taipei might be quickly brought to its knees and forced to capitulate to Beijing.*[12]

Limited PRC cyberwarfare would likely target U.S. logisti the opening salvo of the conflict. The PRC believes both tha U.S. logistical processes are the most vulnerable aspect of military activity, and that U.S. operational vulnerabilities a greatest during the early deployment phase of war. This preemptive approach can be described as part of the Chines strategy of "gaining mastery before the enemy has struck" (*xianfa zhiren*).[13] In this scenario, Chinese cyberwarfare w seek to slow down the deployment of additional U.S. forces required to engage the PLA with overwhelming force in the defense of Taiwan (via misdirection of U.S. matériel stores delay of re-supply efforts). And because of the U.S. aversion casualties and continued belief in the so-called "Powell Doctrine" of only engaging an adversary with overwhelming maximal force required for quick success, the U.S. would no likely engage on a large scale until additional forces were forward deployed and re-supply processes established. This could ultimately buy the PRC an additional week or longer before U.S. military forces were brought to bear, creating a decisive window of opportunity to seize Taiwan and dramatically increase the cost of U.S. involvement.

Assuming such a preemptive scenario is unsuccessful, the PRC could seek to use cyberwarfare more overtly to attack military technologies directly. Such an attack would be focu on the accuracy, timeliness and reliability of information up which U.S. forces depend (i.e., C4ISR systems). This approa was described by PRC scholars in their 2000 Science of Campaigns report:

> *The goal of information warfare is, at the critical time and region related to overall campaign operations, to cut off the enemy's ability to obtain, control, and use information, to influence, reduce, and even destroy the enemy's capabilities of observing, decision-making, and commanding and controlling troops, while we maintain our own ability to command and*

> *control in order to seize information superiority, and to produce the strategic and campaign superiority, creating conditions for winning the decisive battle.*[14]

This tactical application of PRC cyberwarfare is a highly evolved form of Chairman Mao Zedong's dictum that China must "seal up the enemies' eyes and ears, and make them become blind and deaf, and we must as far as possible confu the minds of their commanders and turn them into madmer using this to achieve our own victory."[15] It would effectivel increase Clausewitz's "fog of war" for the U.S., while reduci for the PLA.

Regional conflicts in Asia

PRC cyberwarfare capabilities are not exclusively valuabl a conflict with the U.S. The PRC could find itself in limited wars with a nation other than the U.S., where its current U.S.-focused cyberwarfare capabilities could also prove advantageous.

India is the most likely adversary in such a regional scena Relations between China and India have been marked by political tensions ever since the two countries went to war i 1962 over a still disputed region of the Himalayan border ir Arunachal Pradesh. The PLA was largely successful in defeating the Indian military in that conflict, but skirmishe continued into the late 1980s and the issue remains unsettl today. In the mid-1990s, the PRC and India signed the Sino-Indian Bilateral Peace and Tranquility Accords promo stability along the "Line of Actual Control" in the border conflict.[16] Despite this progress, the PLA maintains a grow presence in the region and many anticipate future conflicts between the two economically rising giants.

India is an increasingly high-tech nation reliant on cyberspace. It has over 60 million Internet users, with its u growth rate exceeding that of China.[17] Much of India's impressive economic growth is due to globalization and the ability to reliably connect to the rest of the world via cybers and IT systems. If the PRC could credibly threaten cyberwarfare against Indian civilian targets in cyberspace, has the potential to succeed in deterring India from opposir interests. If deterrence failed, the PRC would have an effec tool to strike at the heart of India's growth and thus severe erode its will to fight.

Militarily, New Delhi is also vulnerable. While the Indian military is nowhere near as advanced as that of the U.S., it relatively modern fighting force—with all of the vulnerabili that that entails. The PLA could use its cyberwarfare capabilities to leverage those shortfalls as part of a limited regional war. Beyond the Arunachal Pradesh border disput the PRC could covertly or overtly leverage its cyberwarfare capabilities in support of Pakistan during a potential Pakis Indian conflict.

Conflict between China and India will be increasingly like both rise in terms of relative power over the coming decade India develops into an armed power with global aspirations an increasing reliance on cyberspace, the PRC will benefit f being able to hold Indian targets at risk via the threat of cyberwarfare. Such capabilities will not only provide a strat advantage in conflicts with the U.S. and India, but also wit any other modern power with which the PRC comes into conflict.

Total war

The most severe application of PRC cyberwarfare would, f obvious reasons, occur in the context of an unlimited total w with the U.S. Such a conflict would witness the full display all PLA capabilities, both conventional and asymmetric, an potentially even nuclear.

It should be noted, however, that such a scenario is exceedingly unlikely. According to the U.S.-China Economi Security Review Commission, PRC leaders believe future w "will be limited in geographical scope, duration, and politica objectives, and will be highly dependent on command, contr communications, and computer (C4) systems."[18] Yet the catastrophic effects of such a confrontation suggest that, however remote, the scenario warrants examination.

PRC cyberwarfare during total war with the U.S. would include a massive strategic cyberwarfare campaign aimed a U.S. homeland. In 2001, senior analysts at the U.S. Compu Emergency Response Team (US-CERT) and NATO publishe article highlighting the broad and unrestricted nature of su strategic cyberwarfare attack:

> *An unrestricted cyber campaign would almost certainly be directed primarily against the target country's critical national infrastructure: energy,*

> *transportation, finance, water, communications, emergency services and the information infrastructure itself. It would likely cross boundaries between government and private sectors, and, if sophisticated and coordinated, would have both immediate impact and delayed consequences. Ultimately, an unrestricted cyber attack would likely result in significant loss of life, as well as economic and social degradation.*[19]

What would such a campaign look like? Back in 2002, Professionals for Cyber Defense (PCD), a private cybersecu group, assembled a planning team to model a realistic strat cyberwarfare attack on the U.S. Their scenario, called Dark Angel, assumed an attacker would have modest funding ($5 million) and would be focused on destabilizing the U.S. in o to reduce the U.S. ability to project military power and dep the will to fight.[20] The validated Dark Angel attack target rail transportation, oil and gas pipelines, difficult-to-replac power infrastructure, financial service systems, emergency service systems such as 911, and disabled general Internet service.

Chinese cyberwarfare would likely resemble this scenario, without suffering from many of the constraints associated v it. In a total war with the U.S., the PRC would have no nee cloak its actions and would use the full extent of its capabil (well beyond those postulated in Dark Angel). Eliminating these financial and political limitations would allow the PR destroy as much cyber-based infrastructure as possible in a attempt to throw the U.S. economy into chaos, which would simultaneously degrade the U.S.'s ability and will to wage a protracted total war. Such an attack would likely be modele after the reinvigorated concept of "People's War" mentioned earlier. Estimates indicate China has 50,000 Internet police 50,000 military hackers in place or being trained, who will populate over 250 cyber units.[21] Additionally, China has m than a quarter-billion Internet users, many of whom could l employed as patriotic hackers or whose computers could be utilized by the government as part of a Distributed Denial Service attack.[22] All of these individuals could be used in a strategic cyberwarfare first strike meant to cripple the U.S. just as the Japanese attack on Pearl Harbor sought to do decades earlier. The PRC could also augment these efforts v electronic warfare-based cyberwarfare, potentially using

non-nuclear or even nuclear electromagnetic pulse (EMP) weapons delivered by covert means to key infrastructure nc in North America. Furthermore, because computer network and IT systems are extremely interconnected, such an attac would have global consequences.

Strategic cyberwarfare attacks during a total war with the U.S. would destroy critical infrastructure and wreak econor havoc, but their most critical impact may be on the will of t U.S. population. By creating a chronic loss of services such power, emergency response, television and telephony acros U.S., citizens would suffer a loss of confidence in the U.S. government. Individuals would question the status and sec of their personal finances in savings and retirement accoun and uncertainty could lead to rioting and hoarding that wo act as a force multiplier, further stressing an already dama infrastructure. The PRC would be in a position to fuel this chaos further by conducting psychological operations within U.S. through covert means.

Forging a U.S. response

As the discussion above shows, China's interest goes well beyond simply utilizing cyberspace as a tool for espionage. ' PRC is seriously pursuing cyberwarfare capabilities in orde achieve military effects in deterrence, limited war, and tota war scenarios. These scenarios—and PRC cyberwarfare capabilities in general—merit serious consideration by U.S. defense planners and senior leaders.

The U.S.'s response should start with an allied effort to de cyberspace. Such a step is logical; since cyberwarfare is glob in reach, so must be the response. In order to be truly preventive and effective, operations will need to be coordina among many allied states on many different levels. This recommendation was embraced by the U.S.-China Economic Security Review Commission, which stressed in its 2007 re that Congress should "urge the Administration to engage in consultations with its allies on an alliance-based approach China's cyber attacks."[23]

The good news is that multilateral defensive measures sh prove popular with U.S. allies as they would not necessarily require a costly financial investment as do many traditiona military capabilities. Instead, simply granting access and authorities or modifying Information Assurance (IA) tactics techniques and procedures can have a significant impact. T

is welcome news to many NATO members, whose budgets a already spread thin due to changing demographics and cost social safety nets.

Such movement, moreover, is already visible. Following th 2007 cyberwarfare attack on Estonia, NATO began to inves the defense of cyberspace, and Allied nations have more publicly acknowledged the need to secure networks, particu in light of PRC cyber intrusions. These early steps should b augmented by additional ones intended to identify, defend against and defeat future cyber threats on a multilateral le After all, given the unique global nature of cyberspace, isol in confronting cyberwarfare is likely to be even more dange than isolation in the face of traditional threats.

Simultaneously, the U.S. needs to demonstrate a strengthe commitment to defend Taiwan. The current U.S. pledge to defend Taiwan's right to self-determination and independer is ambiguous at best. The Taiwan Relations Act fails to pro a clear security commitment to the island nation, and simp states that any existential threat to Taiwan would be a "gra concern" to the U.S.[24] Some have argued that this vague commitment is helpful because it provides Washington with "strategic ambiguity" necessary to deter any action while providing for a flexible U.S. response. This ambiguity, howe is likely to be interpreted by the PRC as an indication that Taiwan is at the very least less of an essential national pric than was the defense of Europe during the Cold War. Reestablishing an agreement similar to the 1955 Sino-Amer Mutual Defense Treaty would send a strong signal to the P that the U.S. will defend Taiwan, regardless of the PLA's capabilities to inflict harm, in cyberspace or otherwise.

In addition to reducing the possibility of miscalculation regarding the status of Taiwan, the U.S. should undertake effort to develop a declaratory policy which would ensure cl of the costs associated with conducting cyberwarfare agains U.S. and its interests. Such a policy should not only promis retaliation in kind—cyberwarfare in response to cyberwarfare—but also include the full spectrum of military options in response. This would signal to the world that the U.S. is serious about cyberwarfare and truly does consider i par with traditional WMD usage given the scope of the thre U.S. critical infrastructure. Strategic ambiguity may be use in formulating nuclear posture, due in part to the stigma associated with nuclear weapons and their utility in mitiga the conventional Soviet advantage during the Cold War, bu

nature of the cyberwarfare threat requires more explicit guarantees of U.S. military action in response. This policy should also include a provision making it clear that harbori "independent" cyberwarfare attackers is tantamount to the state's launching the attack itself.

The U.S. should also engage in direct talks with the PRC order to ensure total clarity on how the U.S. would respond cyberwarfare. This bilateral dialogue should include discus on important topics such as threat reduction mechanisms, t laws of warfare, and, specifically, how the laws of warfare a to cyberspace and any red lines that may exist.

Perhaps the most obvious recommendation to address the threat posed by Chinese cyberwarfare is to develop and strengthen U.S. capabilities in cyberspace, both of a defensi and offensive nature. Within the United States military, th U.S. Strategic Command (USSTRATCOM) is the global synchronizer for cyberspace operations and is reportedly already pursuing greater offensive capabilities under its Jo Task Force-Global Network Operations (JTF-GNO).[25] Currently, military units from Air Force Space Command (t which the cyber mission was recently reassigned), the developing Navy Cyber Forces Command, and the provisior Army Network Warfare Battalion are working with other U cyberwarfare professionals to establish a durable interagen structure for coordination on cyber threats.[26] Since in cyberspace, even more so than in other domains, the best defense is a good offense, these units, working under U.S.STRATCOM and the JTF-GNO, must continue to devel the tools that could be used to disable the PRC's own cyberwarfare capabilities in the early stages of a conflict.

Finally, the U.S. military must continue to foster flexibilit that will prepare men and women in uniform to adapt and respond if IT processes fail or become unreliable due to a cyberwarfare attack. This effort can be considered a harden of the target of sorts, in this case the actual personnel who the systems dependent on cyberspace. Old fashioned skills utilizing pre-printed field manuals, phones, paper and penc should remain viable, albeit less efficient, avenues to compensate for systems brought down in a cyberwarfare att These "Plan B" tactics, moreover, should be regularly exerc As Secretary of Defense Robert Gates recently cautioned, th U.S. should be modest about what technology can accomplis "…the advances in precision, sensor, information and satell technology have led to extraordinary gains in what the U.S

military can do… But also never neglect the psychological, cultural, political and human dimensions of warfare, which inevitably tragic, inefficient and uncertain."[27] Gates' advic although not focused specifically on cyberwarfare, should be taken to heart by those planning to avert or mitigate a catastrophic electronic attack on the United States.

Taking Chinese cyberwarfare seriously

The threat of cyberwarfare from the PRC is real and growi The U.S. cannot afford to ignore the looming asymmetric th from its rising peer competitor in Asia. There is strong evid that suggests the PRC cyberwarfare threat will increase in sophistication and severity as technology and the offensive advantage outpace cyber defense measures. China's interes cyberwarfare extends beyond intelligence collection into att geared towards both the strategic and tactical disruption of power in order to gain an asymmetric advantage, and Beijin investments in these capabilities is unlikely to diminish. A which makes continued investments by the United States i both offensive and defensive capabilities in cyberspace esse to preserving both U.S. national security and U.S. freedom action within this new domain.

BRIAN M. MAZANEC is a senior intelligence analy SRA International who has supported various agencie within the Intelligence Community, the Joint Staff, th Office of the Secretary of Defense, the Defense Threat Reduction Agency, and the Department of Homeland Security.

1. U.S. Department of Defense, *Annual Report on the Military Power of the People's Republic of China*, 2008, http://www.defenselink.mil/pubs/china.html.
2. U.S. Department of State, International Security Advisory Board Task Force, *Draft Report on China's Strategic Modernization*, September 2008, 1.
3. Qiao Liang and Wang Xiangsui, *Unrestricted Warfare* (Beijing: PLA Literature and Arts Publishing Hou 1999).
4. Richard Lawless, Testimony before the House of Representatives Committee on Armed Services, June 13, 2007, http://armedservices.house.gov/pdfs/FC061307/Lawless_Testimony061307.pdf.
5. William Lord, "USAF Cyberspace Command: To Fly and Fight in Cyberspace," *Strategic Studies Quarterly*, Fall 2008, 8.
6. Bradley Graham, "Hackers Attack via Chinese Web Sites," *Washington Post*, August 25, 2005,

http://www.washingtonpost.com/wp-dyn/content/article/2005/08/24/AR2005082402318.html.

7. John Tkacik, “Trojan Dragon: China’s Cyber Threat,” Heritage Foundation *Backgrounder* no. 2106, February 8, 2008, http://www.heritage.org/research/asiaandthepacific/upload/bg_2106.pdf.
8. Jaikumar Vijayan, “SANS sees Upsurge in Zero-Day Web-Based Attacks,” *Computer World*, Novembe 15, 2006, http://www.computerworld.com/action/article.do?command=viewArticleBasic& articleId=9005117.
9. Dawn Onley and Patience Wait, “Red Storm Rising,” *Government Computer News*, August 21, 2006, http://www.gcn.com/print/25_25/41716-1.html.
10. Cyber Conflict Studies Association, Proceedings of the Annual Symposium “Implication for an Estonia-Like Cyber Conflict for the Government and the Private Sector,” Georgetown University, Washington, DC, February 26, 2008.
11. Richard H. Ullman, “No First Use of Nuclear Weapons,” *Foreign Affairs*, July 1972.
12. James Mulvenon, Testimony before the U.S.-China Economic and Security Review Commission, September 15, 2005.
13. James Mulvenon, Testimony before the U.S.-China Economic and Security Review Commission, May 2 2008.
14. Wang Houqing and Zhang Xingye, eds., *Science of Campaigns* (Beijing: National Defense University Press, 2000).
15. Mulvenon, Testimony, September 15, 2005.
16. Onkar Singh, “India Soft on China’s Arunachal Claim,” rediff.com, November 20, 2006, http://www.rediff.com/news/2006/nov/20jintao1.htm.
17. “2008 Asia Internet Usage and Population Report,” internetworldstats.com, n.d., http://www.internetworldstats.com/stats3.htm.
18. U.S.-China Economic and Security Review Commission, *2007 Report to Congress*, November 2007, 9
19. Timothy Shimeall, “Countering Cyber War,” *NATO Review* 49, no. 4 (2001), 16-18.
20. U.S. Department of State, International Security Advisory Board Task Force, *Draft Report on China’s Strategic Modernization*, September 2008, 3.
21. Mulvenon, Testimony, May 20, 2008.
22. “2008 China Internet Usage Stats as Reported by the China Internet Network Information Center,” internetworldstats.com, n.d., http://www.internetworldstats.com/asia/cn.htm.
23. U.S.-China Economic and Security Review Commission, *2007 Report to Congress*, 139.
24. *Taiwan Relations Act*, Public Law 96-8, 96th Congress, 1979, http://www.ait.org.tw/en/about_ait/tra/.
25. Sean Gallagher, “The Right Stuff for Cyber Warfare,” *Defense Systems*, October 20, 2008, http://defensesystems.com/Articles/2008/10/The-right-stuff-for-cyber-warfare.aspx.
26. Bob Brewin, “Super Cyber Command,” *Government Executive*, October 20, 2008, http://www.govexec.com/story_page.cfm?filepath=/dailyfed/1008/102008wb.htm.
27. Thom Shanker, “Defense Chief Criticizes Bureaucracy at the Pentagon,” *New York Times*, September 2008.