CHINA'S ELECTRONIC LONG-RANGE RECONNAISSANCE

Lieutenant Colonel Timothy L. Thomas, U.S. Army, Retired

Congress passed legislation this week requiring the Pentagon to report on China's growing computer-warfare capabilities when producing assessments of Chinese military power. The fiscal 2008 National Defense Authorization Act, passed yesterday by the House, contains a provision requiring the annual Military Power of the People's Republic of China report to include a new section on Beijing's "efforts to acquire, develop, and deploy cyberwarfare capabilities" in its assessments of China's "asymmetric" warfare capabilities.

—*Early Bird*, 14 December 2007

SINCE 2005, Chinese cyber attacks against U.S. systems have increased at an alarming rate. However, the term "attack" carries unwanted connotations; these unwarranted incursions are more likely reconnaissance missions to collect intelligence on U.S. military systems, to spot vulnerabilities or plant trap-doors or viruses in our systems, and to ensure that China's People's Liberation Army (PLA) has an immediate advantage in the event of war involving America and China. If the incursions were "attacks," then our systems would be down and destroyed. Instead, these computer reconnaissance measures appear to conform to an old Chinese stratagem: "a victorious army first wins and then seeks battle. A defeated army first battles and then seeks victory." Reconnaissance via computer to spot vulnerabilities before the first battle fits the stratagem well.

The United States, of course, is not the only country accusing the Chinese of unwarranted incursions. Germany, England, France, Japan, Taiwan, Australia, and others have also been Chinese targets. When one views these events in the light of open-source accounts of Chinese information operations (IO) theory over the past several years, there is much circumstantial evidence to find China guilty as accused. The only actual forensic evidence, of course, is classified and located in the security agencies of the countries that China has electronically invaded.

This article explains Chinese military thought that supports their cyber-attack activities. While other articles focus on who was attacked and how many times, this article focuses more on the theory behind the attacks, especially the PLA's use of electronic stratagems for their computer network operations and the use of surrogates such as patriotic hacker groups. The article reviews Chinese incursions since 2005 and examines open-source assessments provided by some of the most important Chinese information warfare theorists.

The PLA has followed theory with practice. Computer network operations have become part of the peacetime strategic activities of the PLA. More worrisome is the purpose of these incursions. Is it reconnaissance? Or is the

Lieutenant Colonel Timothy L. Thomas, U.S. Army, Retired, is a senior analyst at the Foreign Military Studies Office (FMSO) at Fort Leavenworth, Kansas. He holds a B.S. from the U.S. Military Academy and an M.A. from the University of Southern California.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
DEC 2008		**00-11-2008 to 00-12-2008**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
China's Electronic Long-Range Reconnaissance	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **U.S. Army Training and Doctrine Command ,Foreign Military Studies Office (FMSO),Fort Leavenworth,KS,66027**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**8**	

purpose of these incursions to place Trojan horses or some other device into U.S. and other partner systems to disable or destroy them in case of war? As one reads about Chinese information warfare developments, it becomes clear that China's potential intentions raise questions.

IW Units and the Active Offense

While the exact reason for China's cyber attacks is unknown, we can follow a cause-and-effect rationale in Chinese contemporary writings. The cause of China's attachment to new information technologies and the "informatization" of their force is the dramatic impact the technologies have had on military affairs, most notably the U.S. use of technology in Iraq. The effect of these technologies on Chinese military thought is the Chinese belief that only countries that take the initiative in an information war or establish information superiority and control ahead of time will win, and that this requires reconnaissance and intelligence gathering before the first battle to set the stage for the use of cyber forces.

Historically, the PLA based its strategic philosophy on "active defense," meaning that China would never attack someone first but would be ready to respond if attacked. That philosophy has changed over the past few years with the advent of the cyber age. There has been a continuous stream of open-source descriptions of both cyber units in and offensive cyber operations by the Chinese military. The PLA's open recognition of a need for offensive operations reflects a significant break with traditional military thought. Further, the PLA has openly stated that U.S. reliance on computer systems is a huge vulnerability ripe for exploitation. If the PLA hopes to offset America's huge advantage in practical application of IO theory (in Kosovo, Iraq, and Afghanistan), it has to exploit that vulnerability. To understand this shift from defensive to offensive-minded operations, we must begin by looking at developments in 1999.

…the Chinese believe that only countries that take the initiative in an information war or establish information superiority and control ahead of time will win…

1999

Nearly a decade ago, Chinese IO theorists were already discussing offensive actions. Zhu Wenguan and Chen Taiyi's *Information War*, published in 1999, contains a section called "Conducting Camouflaged Preemptive Attacks." The authors note that preemptive active offense is needed to disrupt and destroy enemy computer offensive forces.[1] A part of preemption appears to be network surveillance, which involves collecting information on the performance, purpose, and structure of systems related to C4I, electronic warfare, and weapon systems. The authors note that, in the broadest sense, computer information surveillance is a part of computer information attack. They state:

> To conduct computer surveillance, we can use computer information networks set up in peacetime and enter networks as different users to do the surveillance in an area broader than the battlefield. We can borrow the power of computer experts, especially hackers, to finish computer surveillance tasks . . . it can be seen that using hackers to obtain military information from computer networks is a very effective method. We should be familiar with network protocols and accumulate network intelligence.[2]

The authors add that the PLA established small brigades of offensive and defensive computer confrontation forces to conduct these attacks.[3] Offensive training includes how to design and organize virus invasions and how to enter the other side's computer networks. Offensive brigades must repeatedly study and analyze the enemy's potential. They must also be able to sort truth and deception, pinpoint enemy computer-control centers, and jam in targeted ways.[4]

In November 1999, a *Jiefanguin Bao* (*Liberation Army Daily*) article stated that China may develop an information warfare branch of service—a "net force"—to complement the army, navy, and air force. (While the article said this development was very likely to become a reality, there is no evidence to confirm the creation of such a branch of service today.) The force's task would be to protect net sovereignty and engage in net warfare. Elements of net warfare include "offensive and defensive" technologies, "scanning" technologies, "masquerade" (deception)

technology, and "recovery" technology. Masquerade technology would assist a person who wanted to dissemble as a commander and take over a net.[5]

2000

The idea of focusing on reconnaissance and stratagem activities arose as early as 2000. A *Jiefanguin Bao* article notes that units at and above army level should focus their study on reconnaissance and early warning, command coordination, and the application of strategy.[6] An article substantiating this thought appeared in the PLA's authoritative journal *China Military Science* (similar in importance to *Joint Force Quarterly*). The latter article notes that stratagems should create opportunities and favorable times for releasing viruses.[7]

Another *China Military Science* article clarified the offensive posture described in 1999. In it, General Dai Qingmin opines that offense is at least as important as active defense, and notes, "As the key to gaining the initiative in operations lies in positively and actively contending with an enemy for information superiority, China should establish such a view for IO as 'active offense.'" His view is that active offense is essential for maintaining information control, obtaining the initiative, and offsetting an opponent's superiority. Offensive information methods can help sabotage an enemy's information system.[8]

Dai, who became the head of the PLA General Staff's Fourth Department (Electronic Warfare), also notes that IO stratagems can be formulated before launching a war to serve as "a sharp sword" that sabotages and weakens a superior enemy, while protecting or enhancing China's fighting capacity. Information warfare can serve as a type of invisible fighting capacity to evade combat with a stronger enemy.[9] If a future information warfare goal is to defeat strong forces with weak forces using stratagems, then such methods are one of China's asymmetric means to combat U.S. high technology.[10] Stratagems would thus be one of the "magic weapons" that Chinese strategic culture is always stressing.

Finally, Dai's August 2000 article in *China Military Science* discusses the use of electrons as stratagems and the development of an integrated network electronic warfare capability. When combined with the active-offense concept, this article represents one of the most important information warfare articles written in China.

Other less notable publications also discuss offensive operations. In a March 2000 Internet version of *Computer and Information Technology*, analysts at the PLA's Electronic Engineering Institute at Hefei discuss the need for network confrontation teams and the requirement to conduct both defensive and offensive operations.[11] In September 2000, the journal *Guangjiao Jing* noted that the PLA had recently established information warfare departments within its headquarters organizations.[12] Thus, the idea of offensive operations was not limited just to Dai.

2001

The 2001 book *Science of Strategy*, published by China's National Defense University, includes a section on offensive information warfare operations. It states that strategic information warfare should "use offense as a main strategy but be prepared for both offense and defense." Further, it states, "We should use the strategy of the preemptive strike and seize the initiative. Actively launching an information offensive is the key to seizing information superiority and the initiative on the battlefield."[13] In this sense, the thinking appears to apply mainly to wartime and not peacetime action.

The *Science of Strategy* also describes the type of war to fight against networks. The book states that in a war of annihilation, nodes must be attacked to break up the network before attacking weapons systems. Information and support systems must always be the first targets to offset operational balance. *Science of Strategy* notes, "After strikes to damage the net and continuous operations and persistent weakening of the enemy, then vigorously launch an annihilating attack." Ground information warfare facilities, transmission means, reception platforms, and information-flow capabilities should be destroyed in that order. This type of attack enables one to "take away the firewood from under the cauldron."[14] While this scenario appears to apply to wartime conditions, it can easily be adapted to peacetime conditions as well.

Information technology has thus stimulated Chinese strategic thinking; military academics now argue that those who do not preempt will lose the initiative in what may be a very short-lived IO war. In modern conflicts, they suggest, it is easier to obtain the objective of war through one campaign or one battle than at any other time in history. This

line of thinking provides further impetus for the PLA to conduct cyber-reconnaissance activities in peacetime to prepare to "win victory."[15]

2002

An article from June 2002 states that PLA units were prepared to tamper "with information in terms of order, time, flow, content, and form; deleting information in parts, in order to create fragmented information; and inserting information to include irrelevant information in order to confuse and mislead each other."[16] The author adds that two sides in a computer confrontation may attempt to invade each other's information networks by transplanting computer viruses to downloadable software that can be activated when necessary in order to sabotage each other's computer systems.[17]

General Dai Qingmin wrote in 2002 that a priority for the PLA was to acquire offensive information operations equipment, and that the PLA must take and maintain the initiative.[18] Other publications weighed in as well on this point.

Jiefangjun Bao, for example, carried an article in August of 2002 about the forms of network attacks. These were listed as "premeditated" (i.e., a persistent computer virus embedded in software), "contamination" (aimed at the quality of information), "strong" (refering to the forced modulation of computer viruses into electromagnetic waves), and "fission" (the strong regeneration capability of a virus).[19] All are capable of being inserted in peacetime, except perhaps the "strong" variety.

2003

At the 2003 10th National People's Congress, PLA representatives revealed that it would activate the first high-tech information warfare units in Beijing that year. The report stated that the units would eventually be in all PLA armies. Information warfare units would be outfitted with high-tech equipment, and have the ability to conduct network warfare on the Internet and the capability to transfer data via remote sensing satellites.[20] How the "first" information warfare unit differs from the information warfare brigades under discussion in the 1999 Chinese book *Information War* is unknown.

General Dai, writing in 2003, stressed once again the importance of carrying out information attacks.[21] Dai wrote that information warfare is "precursory" (begins before other operations) and "whole course" (runs throughout an entire operation). Perhaps the current emphases on gaining the initiative and on short wars are the main reasons that Dai gives the impression that preemption via information warfare is a necessity in future war.[22] He notes:

> Actions such as intelligence warfare, psychological warfare, and campaign deception in advance of combat seem to be even more important to the unimpeded implementation of planning and ensuring war. For this reason, information warfare must be started in advance of other combat actions before making war plans and while making war plans.[23]

Specific reserve units also engage in information warfare activities. For example, in late 2003 the monthly journal of the PLA Academy of Military Science, *Guofang*, gave specific instructions on network attack activities to reserve units. Author Li Mingrang says that information storm troopers as "first forces" must be established from the talent of local communications, telecommunications, and financial departments and from scientific research institutes and institutions of higher education. Stratagems must be developed to increase system survivability.[24] Li adds:

> There is no shortage of computer experts and network jockeys among them, any one of whom could become a network guerrilla who could open up a gunpowderless battlefield all by himself by harassing attacks on the network, namely by releasing large volumes of data from many directions concentrated on some enemy network station to jam up its network router and bring the network station to a standstill…and once there is a military requirement, either enter the network system to steal intelligence or to activate viruses or detonate 'bombs' to achieve the combat target of destroying the network.[25]

Reserve forces are directed to work on offensive strategies.

In his 2003 book *Deciphering Information Security,* China's "father of information warfare," retired Colonel Shen Weiguang, wrote about the development of an information security university with a military information security specialty. The specialty

teaches, among some twenty-plus topics, "A Study of Hacker Attack Methods," "Network Intrusion Detection and Defending against Attack," "Information Attack and Defense Tactics," "Computer Virus Program Design and Application," "Network Security System Structures," and "Scanning for Hidden Troubles in Networks."[26] Many of these topics would fit the definition of PLA's peacetime computer network operations incursion activities.

2005

In the 2005 book *Study Guide for Information Operations Theory*, General Dai and his associates defined 400 IO-related terms, many related to preemptive or reconnaissance activities. Only computer network warfare is described here:

> Computer network warfare is composed of computer network reconnaissance, computer network attacks, and computer network defense. Operations mainly involve the use of armed and equipped network warriors. The means of operations include various types of viruses, logic bombs, and chip weapons developed from computer technology. Computer network warfare will act as both a deterrent and a means of warfare, and it can have a large and profound impact upon the enemy's politics, economics, and military. It is also an important means of battle for a less well-equipped military against one with formidable strengths in high technology.[27]

Dai also discussed the importance of the conduct of warfare, focusing on information deterrence as a concept to consider and develop further at the strategic level. Others who have written on the topic of information deterrence include Shen Weiguang. The book *Science of Military Strategy* devotes an entire chapter to the topic. The latter source explains how information deterrence (intimidating by demonstrating one's information power or might) can help achieve national and military objectives. Deterrence methods include information technology (hardware and software innovations), information weapons (discursive dissimulation or disinformation), and information-resource suppression (analogous to jamming). According to some Chinese authors, counter-information deterrence theories must also be considered.

In *Warfare Strategy Theory* (2005), Yao Youzhi asserts that strategy has developed to the point where technological considerations dominate and the use of technology has become strategic. Any strategy that distances itself from focusing on high-technology weapons has no useful value, according to Yao. This also means that China must develop sound counterstrategies.[28] He writes:

> It is necessary to be proficient at utilizing the information superhighway, creating misleading information, spreading the fog of war, and jamming and destroying the enemy's strategic awareness, thereby using strategy to control the adversary. It is necessary to be proficient at using electronic feints, electronic camouflage, electronic jamming, virus attacks, and space satellite jamming and deception, leading the enemy to draw the wrong conclusion and attaining the goal of strategic deception.[29]

While designed for wartime use, several of these techniques work as peacetime preventive and preemptive measures as well.

In "stovepipe" structured commands of the past, a force calculated its strength by adding together all of its parts. Today, a force's combat strength is a product of operational elements where information technologies factor into a potentially exponential multiplication.[30]

Yao writes that "informationized" warfare has changed the traditional significance of "attack, capture, control, and defend" because precision attacks have made possible the destruction of the enemy's entire war system. The primary attack target has become an enemy force's strategic information system. All activities now revolve around gaining battlefield supremacy, and information supremacy is the foundation of battlefield supremacy. Directly destroying an enemy's will has supplanted the annihilation of an enemy's military capability. This focus on information invites completely new methods in future wars.[31]

2007

Author Zhang Zhibin notes in *Jiefanguin Bao,* 13 March 2007, that the dialectical relationship between offense and defense in network warfare must place equal emphasis on each. A network deterrence theory implies that both capabilities are necessary,

AP Photo, Andy Wong

A computer screen displaying a military website is seen inside an army base in Tianjin, on the outskirts of Beijing, China, 30 July 2007. Computer networks have been targeted by cyber spies that media reports say are directed by China's military, but China denies backing such attacks.

offense to scare any potential enemy force, and defense to thwart any attack. Zhang says:

> Only by doing a solid job of positive defense can China ensure winning the initiative in network warfare. Thus, China should make unremitting efforts to seek such preemptive opportunities through developing network technology and systems and making corresponding network defensive operations research and implementation.[32]

Other articles from 2007 stress a need for PLA action to gain network control, including access, if possible. Two books on Chinese IO by this author, *Dragon Bytes* and *Decoding the Virtual Dragon,* mention this focus on control.

…information supremacy is the foundation of battlefield supremacy.…This focus on information invites completely new methods in future wars.

Probable Chinese Computer Attacks against America

Over the past several years, Chinese information warfare and IO capabilities have become more visible and troubling. China has used these capabilities not only against the U.S. but reportedly against Japan, Taiwan, Germany, England, and Australia as well. Due to the nature of computer network operations, exactly how many Chinese information warfare reconnaissance or offensive events have transpired or the actual intent of these incursions remains unknown. Those episodes that have leaked into the public domain include the following:

- Espionage conducted against the U.S. Department of Defense computers, reported in *Time* magazine. The report concerned a Chinese cyber espionage ring that federal investigators codenamed Titan Rain.[33]
- Chinese attempts to blind a U.S. satellite, reported in *Defense News*. The report discussed high-powered Chinese laser attacks on a U.S. satellite.[34]
- Chinese hacker attacks on the U.S. Naval War College's net capability, reported in *Federal Computer Week.* This attack purportedly originated from China and took systems off-line.[35]
- The Chinese destruction of an old Chinese weather satellite with an anti-satellite missile, reported on National Public Radio. The report cited a Beijing People's University commentator. He noted, "Satellite-killing technology is logical in the development of missiles and an information warfare capability."[36]
- A sophisticated computer attack on Tennessee's Oak Ridge National Laboratory in October and November 2007. The assault was in the form of phony e-mails which, when opened, allowed hackers to penetrate the lab's computer security.[37]
- Hacker attacks against Japan and Taiwan, reported in the Japanese and Taiwanese press.[38] The reports noted that these attacks were retaliations for Japan's anti-Chinese interpretations of history and for Taiwanese claims for independence.

On 5 September 2007, the *Kansas City Star* carried an article in which China denied cyber-attacking any country. Foreign ministry spokesperson Jian Yu noted, "The Chinese government has always opposed an Internet-wrecking crime, including hacking, and cracked down on it according to the law."[39] He dismisses accusations of Chinese attacks

on Pentagon computers as "groundless." A Pentagon spokesperson refused to say if the perpetrator was China, but Britain's *Financial Times* quotes an unidentified senior U.S. official as saying the source had been traced to the PLA.

A week earlier, Germany's *Der Spiegel* magazine reported that the PLA had infiltrated Germany's government computer systems. The report said the hackers had been traced back to Guangzhou and Lanzhou.[40] Thus, circumstantial evidence continues to grow. It is difficult to believe that Germany, Australia, Japan, Taiwan, and America are all conniving to indict China and portray it as a new threat. Indeed, through unprovoked cyber operations, China seems to have indicted itself without anyone's assistance.

China's Use of Surrogates

One of China's stratagems is to "attack with a borrowed sword." Perhaps the use of patriotic hackers fits this stratagem. A recent article in *Time* magazine discussed the use of a "network crack program hacker" (NCPH) group initiative to accomplish this goal. The article said the PLA had developed a competition for hackers and that the winner would receive a monthly stipend from the military. It noted that the NCPH group not only won the competition and received the stipend, but the PLA also used the NCPH to teach techniques and procedures to other members of the PLA's cyber-warfare team. A U.S. branch of VeriSign, iDefense, has noted that China's NCPH created 35 programs to implant Trojans (which take partial control of computers) and that these programs attacked U.S. government agencies. VeriSign's iDefense accused the NCPH of siphoning off thousands of unclassified U.S. documents. Such activity would fit the PLA's preemption focus.[41]

The concept of "people's war" also fits with so-called patriotic hacking. "People's war" in the cyber age means that citizens get involved with hacking or cyber attacking an enemy's systems. Presently over 250 hacker groups operate in China.[42] Quantity could thus create a quality all its own with the variety and intensity of incursions they could conduct. None could be traced directly to the PLA if hacker groups are private citizens (or for that matter, military members or military reservists conducting cyber operations from their home computers). Again, circumstantial evidence is all that one has to go on, but that evidence is becoming overwhelming.

One of China's stratagems is to "attack with a borrowed sword." Perhaps the use of patriotic hackers fits this stratagem.

Conclusions

Chinese theory over the last several years indicates that China wants to become proficient in active offense, cyber reconnaissance, cyber-stratagem, and computer exploitation activities in case the PLA has to go to war. If China feels it can gain the initiative by obtaining information superiority or by preventing cyber strikes, then the coming years may involve challenges from that sector. While it remains easy to measure the intent of troop deployments, the intent of a Chinese electron is harder to measure. Is it inserting a virus, conducting reconnaissance, or disabling a system? The world will move into uncertain territory as nations attempt to conduct responses to and develop consequence management actions for truly disruptive electronic intrusions.

The Chinese note that IO tactics and techniques allow more emphasis on the principle of offense than on traditional warfare. A weaker force, for example, can inflict much damage on a superior force with a properly timed and precisely defined asymmetric information attack. China portrays itself regularly as the weaker side of the U.S.-Chinese relationship. It thinks that offensive operations such as information deterrence, information blockade, information power creation (electronic camouflage, network deception, etc.), information contamination, information harassment, nodal destruction, system paralysis, and entity destruction are key to victory in a modern conflict with America.

One should remember that this analysis stems only from open-source information and public comments from the PLA, and that China's understanding of the intersection of strategy and information technology, especially as it relates to actual conflict, is not extensive in a practical sense. The

Chinese have little recent experience with conflict. Their forces have not fought an actual war in decades. From a theoretical perspective, however, China has written extensively on the use of information technology and electronic preemption and given both much thought. Chinese cyber intrusions indicate that the Chinese are gaining a lot of practical and theoretical experience in peacetime.

The PLA's open-source comments can be interpreted either as an attempt to work with the West or to vigorously oppose it. Perhaps the PLA is being very open and transparent in its cyber strategies, perhaps more open than in any other area of military operations. (The PLA is far more open with its information warfare thinking, for example, than Russia.) If the PLA's intent is to oppose the West, it may in fact be concealing rich information warfare concepts in PLA "rules and regulations" (the PLA's equivalent of doctrine) within the general staff directorates and research institutes. China's information warfare rules and regulations are not available to other nations, while unclassified U.S. doctrine is available to anyone on the Internet. The PLA keeps its rules and regulations close to its chest. In this case, lack of transparency introduces unwanted ambiguity. America and other nations under threat of PLA incursions may react harshly to some scenarios developed by the Chinese and, thus, unintentionally set off a conflict.

How and when China might use its active-offensive concepts for purposes other than reconnaissance is unclear, but, as general concepts, they are worrisome. It does not bode well for future cooperation and stability if Chinese theorists really do believe (as they openly state) that China can offset an opponent's information superiority only if China strikes first. China will no doubt continue to use technology in conjunction with innovative stratagems to try to deceive our high-tech systems or perhaps even to force errors in the cognitive processes of U.S. decision-makers. We live in interesting times. ***MR***

NOTES

1. Zhu Wenguan and Chen Taiyi, *Information War* (place and publisher not stated, 1999), chap. 5 (Computer Operations). This chapter discusses offensive and defensive computer operations.
2. Ibid.
3. Ibid.
4. Ibid. At one point in the discussion, the authors state, "We need to observe our military's strategy of active offense and in computer confrontation training ensure both defense and offense are main partners."
5. Leng Bingling, Wang Yulin, and Zhao Wenxiang, "Bringing Internet Warfare into the Military System is of Equal Significance with Land, Sea, and Air Power," *Jiefangjun Bao* (*Liberation Army Daily*), 11 November 1999, 7, as translated and downloaded from the Foreign Broadcast Information Service (FBIS) Web site, 15 November 1999.
6. Fan Changlong, "Stand in the Forefront of the New Military Revolution in Deepening Troop Training through Science and Technology," *Jiefangjun Bao* (*Liberation Army Daily*), 4 April 2000, 6, as translated and downloaded from the FBIS Web site, 6 April 2000.
7. Niu Li, Li Jiangzhou, and Xu Dehui, "Planning and Application of Strategies of Information Operations in High-Tech Local War," *Zhongguo Junshi Kexue* (*China Military Science*) no. 4, 2000, 115-22, as translated and downloaded from the FBIS Web site, 9 November 2000.
8. Dai Qingmin, "Innovating and Developing Views on Information Operations," *Zhongguo Junshi Kexue*, date not given.
9. Ibid.
10. Ibid.
11. Yang Jian, Zhang Youhua, and Lu Zhankun, (no title), *Jisuanji Yu Xinxi Jishu* (Internet version of *Computer and Information Technology*), Anhui Computer Subscriber Association and the Anhui Computer Society, 16 March 2000, as translated and downloaded from the FBIS Web site, 18 April 2000.
12. "China's IW Capabilities," *Guangjiao Jing*, Hong Kong, 16 September 2000.
13. *Ge Zhenfeng*, chap. 16, sec. 4, 366. For translations of excerpts of this book, the author thanks Dr. Gary Bjorge, Combat Studies Institute, Fort Leavenworth, Kansas.
14. *Ge Zhenfeng*, chap. 24, sec. 6, 493.
15. Peng and Yao, 418-19.
16. Wen T'ao, "PLA Bent on Seizing 'Information Control.'" *Hong Kong Ching Pao*, 1 June 2002, no. 299, 44-46, as translated and downloaded from the FBIS web page, 5 June 2002.
17. Ibid.
18. Dai Qingmin, "On Integrating Network Warfare and Electronic Warfare," *Zhongguo Junshi Kexue* (*China Military Science*), February 2002, 112-17, as translated and downloaded from the FBIS Web site, 24 June 2002.
19. Fan Yongsheng, Wu Xinghan, "War on Networks: Modern 'Contradictory' Offensive, Defensive Warfare," *Jiefangjun Bao* (*Liberation Army Daily*), 14 August 2002, 11, as translated and downloaded from the FBIS Web site, 14 August 2002.
20. "PLA to Organize First Information Warfare Units," *Mingpao News*, 12 March 2003, <http://full.mingpaonews.com/20030312>.
21. *Direct Information War*, 170.
22. Ibid., 169.
23. Ibid.
24. Li Mingrang, "Develop the Advantage of People's War under the Conditions of Innovation and Informatization," *Guofang*, 15 November 2003, 7-8, as translated and downloaded from the FBIS Web site.
25. Ibid.
26. Shen Weiguang, *Deciphering Information Security* (Xinhua Publishing House; July 2003), 127-241.
27. Ibid., 211.
28. Yao Youzhi, Editor-in-Chief, *Warfare Strategy Theory* (Liberation Army Press, 2005), 475-76.
29. Ibid.
30. Ibid., 346-49.
31. Ibid., 99-101.
32. Zhang Zhibin, "Offense is Not Necessarily the Best Defense—Preliminary Study and Thinking on the Dialectical Relationship between Offense and Defense in Network Warfare," *Liberation Army Daily*, 13 March 2007, as downloaded from the Open Source Center web site, 9 April 2007.
33. Nathan Thornburgh, "The Invasion of the Chinese Cyberspies," *Time*, 29 August 2005, <www.time.com>.
34. Vago Muradian, "China Tried to Blind U.S. Sats with Laser," *Defense News*, 25 September 2006, 1.
35. Josh Rogin, "Network Attack Disables Naval War College," *Federal Computer Week*, 30 November 2006, <www.fcw.com>.
36. Anthony Kuhn, *National Public Radio*, 19 January 2007, interview with Beijing representative.
37. "Oak Ridge National Lab Reports 'Sophisticated' Cyber Attack Netted Personal Data on Visitors," The Associated Press, 6 December 2007, <www.iht.com/bin/printfriendly.php?id=8626732>.
38. "Chinese Hackers Attack Taiwan Military Computers," *Taipei P'ing-kuo Jih-pao* (Internet Version), 15 May 2006, as reported in Open Source Center report CPP20060516310002.
39. Tim Johnson, "China Denies Cyber-Attack," *Kansas City Star*, 5 September 2007, A5.
40. Ibid.
41. Simon Elegant, "Enemies at the Firewall," *Time*, 19 December 2007, <www.time.com/time>.
42. Conversation with Scott Henderson, whose book on Chinese hackers, *Dark Visitor,* is forthcoming. This book is probably the best open-source work on Chinese hackers.