Google Confronts China's "Three Warfares"

TIMOTHY L. THOMAS

In early January 2010, Google announced that a computer attack originating from China had penetrated its corporate infrastructure (in mid-December) and stolen information from its computers, most likely source code. The hackers also accessed the Gmail accounts of some human-rights activists and infiltrated the networks of 33 companies. In April 2010, journalist John Markoff wrote:

> A person with direct knowledge of the investigation now says that the losses included one of Google's crown jewels, a password system that controls access by millions of users worldwide to almost all of the company's Web services, including e-mail and business applications. The program, code named Gaia for the Greek goddess of the earth, was attacked in a lightning raid taking less than two days last December, the person said.[1]

China's recent incursions into US military computer networks and Google's cyber systems are of concern when viewed in isolation. They reflect a more serious problem when viewed as part of a short-term goal of conducting "preemptive reconnaissance" that accommodates a longer-term goal of affecting US military planning or the US economy. Many factors indicate that this may be China's goal.

Initially, this article examines the context within which the Google attacks occurred and how Google's response—abandoning censorship in China—was used by the Chinese to distract attention from their planned aggression. It then analyzes how a 2003 military regulation assisted China's response to Google's accusations. In short, these procedures are being used all too often by the Chinese and are causing US authorities to be more and more intolerant of Chinese behavior.

Timothy L. Thomas is an analyst at the Foreign Military Studies Office at Fort Leavenworth, Kansas, and the author of three books on Chinese information warfare.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2010		**00-00-2010 to 00-00-2010**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Google Confronts China's 'Three Warfares'	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 War College,ATTN: Parameters,122 Forbes Avenue,Carlisle,PA,17013**	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)**	**13**	

Why America Has Had Enough

Journalist Josh Rogin recently listed ten computer incidents that are commonly known in the United States through press releases and government agency briefings. All parties damaged by the attacks suspect that the Chinese are behind these incursions. The ten events are:

• 2004: Titan Rain, Federal Bureau of Investigation name for a group of hackers from Guangdong province who stole information from US military labs, the National Aeronautics and Space Administration, the World Bank, and others.

• 2006: A US State Department official in East Asia opens an e-mail that allows hackers to break into computers at US embassies all over the region.

• 2006: US Representative Frank Wolf's office is attacked. He is an outspoken lawmaker on Chinese human-rights issues and suspects the Chinese in the attack.

• 2006: The US Commerce Department had to discard all of its computers due to targeted attacks originating from China.

• 2006: The US Naval War College took all of its computers offline after a major cyber attack in which China emerged as the main culprit.

• 2007: Secretary of Commerce Carlos Gutierrez finds spy software on his computer following a trade mission trip to China.

• 2008: The presidential campaigns of both President-elect Barack Obama and Senator John McCain are attacked by Chinese cyber spies.

• 2009: Senator Bill Nelson revealed attacks against his computer had been traced to China.

• 2009: Toronto researchers find a massive cyber espionage ring using Chinese malware they call Ghostnet. The attacks penetrated 103 countries, and their origin was China.

• 2009: Lockheed Martin's F-35 program is hacked and China emerges as the main suspect.[2]

This list obviously does not include the hundreds of thousands of "pings" (purpose unknown) that US Web sites have received from China over the years, nor does it mention other specific incidents. And then along comes Google.

How Serious was the Google Attack?

The attack on Google occurred in December 2009. Some sources state that as many as 33 companies were victims of the hack attack.[3] Alan Paller, the director of the well-known information security training firm known as the SANS Institute in Bethesda, Maryland, indicated just how invasive the

attacks were, noting "the odds of the 25 biggest companies in California not being fully compromised by the Chinese is near zero."[4] His analysis indicates the probes were serious and highly effective. Fully compromised? One hopes that Paller was exaggerating the threat, but there are many reasons to believe he was not.

The Chinese are looking as closely at economic secrets as they are military or diplomatic secrets.

The attack itself on Google was so out of context, so odd, that US Chinese cyber expert James Mulvenon called the event a "watershed moment in the cyber war."[5] Perhaps this was because the attack focused on commercial firms, which had appeared to be a secondary option of the Chinese in past attacks. Or perhaps it was because this was the first time a commercial firm, Google, had actually come forward and admitted they were under attack. Past practices had witnessed commercial companies and banks remaining quiet when experiencing cyber attacks in an attempt to retain consumer confidence. The Pentagon, on the other hand, has been quicker to move and announce probes against their systems.

Acts of commercial espionage indicate that the Chinese are looking as closely at economic secrets as they are military or diplomatic secrets. Perhaps, after the thousands of attacks already attributed to China, Chinese hackers have accomplished everything they wanted in government spheres and have moved on to bigger prizes. Or perhaps they simply have decided to alter their target methodology. In addition to Google, Adobe Systems, Rackspace Hosting, and the Santa Barbara, California, software maker CyberSitter all reported attacks.[6] Sometime later, the law firm Gipson Hoffman & Pancione (representing CyberSitter and Symantec), Juniper Networks, Northrop Grumman, Yahoo, and Dow Chemical reported hits by the attackers.[7]

A few months earlier, Northrop Grumman had published a report that outlined various Chinese computer exploitation activities. The report was written at the behest of the US-China Economic and Security Review Commission. It indicated that Chinese activities against commercial firms have been ongoing for quite some time. In particular, the report detailed an extensive Chinese-based cyber mission conducted against an unnamed US commercial firm a few years earlier. During this espionage case, the Chinese utilized an extensive reconnaissance plan against the company that continued over a number of months. Evidence suggesting a thorough reconnaissance effort can be implied from the attackers' actions once the actual intrusion plan unfolded. The perpetrators did not open and review files but, due to their successful reconnaissance effort, simply began to copy and remove the files or folders they wanted. Their reconnaissance activities were

so precise they were successful in stealing the information they sought. A break-in of this nature could only have occurred after an accurate map was made of the targeted network and files.[8]

When the time came to break into the company's computer network, the cyber thieves utilized breach teams, collection teams, exfiltration teams, and intermediate "staging servers" to accomplish their mission. The Northrop Grumman report notes that "the exfiltration operation indicates that their command and control architecture relied upon previously stolen valid user accounts to breach the company's internal servers."[9] This was a sophisticated effort that acquired specific intellectual property.

Google responded by threatening to remove its censorship of certain items from its Chinese network. This infuriated the Chinese and allowed them to accuse Google of evading Chinese law. Eventually, Google moved the focus of their Chinese Internet activities to Hong Kong.

Who Attacked Google?

On 18 February, David Barboza and fellow journalist John Markoff questioned who might have committed the Google probes. Their primary finding pointed to China although they offered other potential scenarios as well.

Initially, the journalists noted the US National Security Agency and other computer-security firms traced the attacks to servers in Taiwan. Then citing "people involved in the investigation," they reported that the attacks were traced to two educational institutions in China. The journalists reported that a US defense contractor that had attacks similar to those that Google experienced had identified an unusual suspect, a Ukrainian professor teaching at a Chinese vocational school, as the source behind the attacks.[10]

The Chinese institutions involved were identified as the Shanghai Jiaotong University and the Lanxiang Vocational School. The journalists noted that these institutions may have been used as fronts for government agencies.[11] Markoff and Barboza also conferred with Mulvenon and discovered that the Chinese have a different model for computer network exploitation operations. These operations incorporate volunteer "patriotic hackers" in support. Other Chinese experts told the journalists that China has a highly distributed approach to online espionage that makes it impossible to prove where attacks originate.[12]

An interesting part of the article was the journalists' ability to conduct interviews with two Chinese professors at Jiaotong University. One professor said that an internal investigation at the university had already started. The other said it was possible someone from the university was involved since an individual could commit an act of wrongdoing, or possibly

the university Internet Protocol address was hijacked. Jiaotong is no ordinary university. It has ties with several US universities, to include Duke and the University of Michigan, and to various US commercial entities such as Microsoft and Cisco Systems. Jiaotong received funding from Chinese Project 863 (China's Information Technology Security Plan), has a School of Information Security Engineering, and has People's Liberation Army ties, according to the university's Web site. It has also hosted prominent Chinese hackers for lectures.[13] At least one of these hackers is antiwestern and believed to have previously worked for Google.

A representative from the other school, the Lanxiang Vocational School, said he doubted whether any of the high school graduates at his school had the ability to hack Google or any other company. This may be a bit of an understatement since the school's computer laboratory is so enormous that it was listed in the *Guinness Book of World Records*. The school's Web site states that it sends a number of graduates to the armed forces. The school's dean, Mr. Shao, said graduates of the school's computer science department are recruited by the local military on an annual basis.[14]

Barboza and Markoff added that other computer industry executives (and former government officials) said it "was possible that the schools were cover for a 'false flag' intelligence operation being run by a third country."[15] Or perhaps, the attacks were the responsibility of criminal elements dealing in industrial espionage.[16] Thus, at the end of their article, the reader is wiser but still not certain as to who committed the attacks. The majority of the evidence, however, indicts China.

Chinese Responses to Google's Accusations

Based upon the number of nations (Germany, India, Taiwan, Canada, Australia, and England, among others) that have accused China of Internet attacks, Chinese spokespersons have plenty of practice at denying their nation's involvement in cyber exploitation activities. These government representatives have developed a standard, almost predictable, response. In many respects the responses follow new military *Regulations on Political Work* provided to Chinese propaganda specialists in 2003. This regulation was written after China observed how the United States and its Coalition partners used information during the intervention in Iraq. Possibly, civilian propaganda agencies were given the same information. Chinese political-military commissars were instructed as to how individuals should explain events via the conduct of media warfare, legal warfare, and psychological warfare in times of peace and conflict.

Chinese regulations note that it is the media's job to support a righteous cause, the legal expert's job to justify the cause, and the psychological

warfare personnel's job to bolster friendly morale while attacking the enemy's morale. This is how the media can be used to control public opinion and eliminate any chance of China "losing face." The "three warfares" permit China to enter any fray, whether in peace or war, with a political advantage that can be used to alter public or international opinion.

An analysis of the aftermath of the Google probes provides an example of this process. The initial Chinese responses to Google's accusations were offered by many of the same agencies that the Chinese have used in the past. Initially, a Foreign Ministry spokesman (Ma Zhaoxu) said, "foreign enterprises in China need to adhere to China's laws and regulations, respect the interests of the general public and cultural traditions, and shoulder corresponding responsibilities. Google is no exception."[17] Ma did not indicate that China would investigate Google's accusations nor did he mention the grounds for Google's decision to remove censorship, namely that someone in China had attacked its infrastructure. Chinese authorities dismissed the accusations as groundless. Psychologically, Ma used the stratagem of diverting attention away from the real issue under consideration, the probes, and redirected the focus to various legal issues.

The real issue at stake is that the Chinese were accused of stealing source code and conducting espionage (or stealing proprietary information) from 33 companies. The initial accusation of espionage is more important than China's after-the-fact accusation that Google was violating China's rules and regulations regarding censorship. Google did not violate rules and regulations before the event. It followed Chinese law. It stated that it would violate its censorship agreement only after the probes on Google's systems transpired and the Chinese refused to take responsibility or aid in finding the culprit. Secretary of State Hillary Clinton made a strong diplomatic statement in support of Google, stressing many of the same issues.

And what was the Chinese response to Secretary Clinton's statement? The Zhaoxu news agency said Clinton's singling out China was inappropriate and misguided and constituted an inappropriate meddling in Chinese affairs.[18] Again, who was meddling in whose affairs? Another Foreign Ministry spokesman, Jiang Yu, said, "China's Internet is open" and China "welcomes international Internet corporations to do business in China in line with the law."[19] Such subjective responses are specifically designed to undermine the accuser's line of reasoning.

Next, in typical Marxist-Leninist fashion, the Chinese relied on the old "counterpoint" tactic from the Communist playbook. Google accused the Chinese of collecting data on human-rights advocates, so China accused the United States of human-rights violations in one of its responses. Then, since Google and other US journalists implied Chinese government collusion in the espionage activities, the Chinese next implied White House collusion

in using commercial markets (such as Google) for political purposes, yet another counterpoint tactic. A *China Daily* Internet commentary noted that four of Google's former executives hold positions in the US government, to include Sumit Agarwal, now a Deputy Assistant Secretary of Defense for Public Affairs Outreach and Social Issues.[20] The commentary went on to note that Google was the fourth-largest contributor to President Barack Obama's presidential campaign. Counterpropaganda today is perhaps an element of what might be termed soft psychological power.

Foreign Ministry spokesmen were not the only ones to address Google's accusations against the Chinese. Several military officials also joined in the renunciation and diversion. Huang Xueping, a Defense Ministry spokesman, stated that Google's claims were baseless, irresponsible, and hyped with ulterior motives.[21] Li Daguang of National Defense University stated that some western powers had adopted a strategy to sabotage China's information technology development and that their high-profile criticism is a preemptive strike on China.[22] Li Yizhong, Minister of Information and Technology, stated that Google must obey China's laws and that China opposes hacking.[23] While many more defensive accusations were levied at Google, the three mentioned here represent the categories of media, psychology, and law. Other sources used to put out the official propaganda ranged from representatives of the Academy of Military Science to publications such as the *Central Party School*.

In addition, other propaganda materialized two months after Google's initial accusations and involved the imposition of strict control over Chinese media outlets. Two major groups were targeted: editors and mangers, along with monitoring and control groups.

When addressing Google issues, chief editors and managers of Chinese propaganda outlets were told to use only central government media content; not to change titles when reposting; not to produce relevant topic pages, discussion sessions, and related investigative reports; not to permit forums and blogs to hold discussions or investigations on Google; to clean up text that attacks the Party, state, government agencies, and Internet policies or sites that support Google; and to monitor Google information and incidents.

Monitoring and control groups were told to immediately conduct follow-up and control actions; not to participate in Google's information releases; not to report that Google is exerting pressure on China; and not to provide materials for Google to attack relevant policies.[24] Such instructions are representative of standard Chinese propaganda practices.

David Berlind, writing for *InformationWeek*, felt the US response (excluding Secretary Clinton's) to Chinese actions was "wimpy." He wrote that the response indicated that the United States fears China since the latter

now holds a winning hand for four reasons: the United States needs China to support our growing national debt; we need China to manufacture much of what we consume; we depend on the growth of China's economy for our growth since we have little domestic production; and we need China to keep North Korea in line.[25] The longer western nations take to send a strong message to the Chinese, the more credible Berlind's accusation appears. Secretary Clinton's initial response was the quickest and most pointed to date.

Chinese Thinking Adapts to the Digital Age

Several classical Chinese stratagems fit the latest Internet behavior and indicate possible trouble in the future. A stratagem is an action or plan designed to mislead an adversary's perception, thinking, emotion, or will. In nearly every case stratagems attempt to divert an opponent's attention and lead them down an incorrect logic path. Stratagems support Sun Tzu's dictum that "all war is deception."

The constant reconnaissance efforts that China conducts against countries around the globe indicate that China, along with developing new technologies, is trying to fulfill the stratagem of "win victory before the first battle," that is, find the vulnerabilities in another system and be ready to exploit them. This type of activity could lead to a military victory in time of conflict or result in an economic victory. The reconnaissance activities reported by Alan Paller against the 33 largest companies in California serve as a good example of these types of activities. Securing an economic victory would also fulfill the stratagem of "win victory without fighting." Chinese actions over the past several years seem to accommodate this stratagem. China espouses a policy of peace and kindness while continuing to conduct persistent cyber attacks, that is "make noise in the west, attack in the east." Finally, the constant repetition of the slogan that China is developmentally way behind the United States and other western nations fulfills the stratagem "appear weak when strong."

Chinese reconnaissance activities are aggressive and intrusive, a stark departure from its more traditional military strategy that focused on the active defense. Digital-age practices have resulted in greater emphasis on the offensive and attaining the initiative. Now, while emphasizing peaceful rhetoric, the Chinese also talk openly about acquiring advantages. The military has been particularly aggressive in this respect, pursuing both the theory and practice of information warfare activities. The People's Liberation Army has manifested this tendency by seeking preemptive opportunities via the reconnaissance of other nations' network technologies whenever possible.

Prominent US officials have taken note of this offensive behavior and pointed their cyber-espionage finger directly at China. In November 2007 testimony before the US-China Economic and Security Review Commission, General James Cartwright, then Vice Chairman of the Joint Chiefs of Staff, blamed China for cases of cyber-espionage. He was particularly concerned about China's use of denial-of-service attacks.[26] During Cartwright's testimony, he stated:

> The data collected from these computer reconnaissance campaigns can be used for myriad purposes, including identifying weak points in the networks, understanding how leaders in the United States think, discovering the communication patterns of American government agencies and private companies, and attaining valuable information stored throughout the networks.[27]

Both civilian and military Chinese sources have written about this growing cyber offensive, particularly regarding its economic nature. The journal *China Military Science* has devoted a number of articles to topics associated with Internet warfare and China's interest in developing offensive cyber options. In 2009 Senior Colonel Wang Wei, a professor at the Nanjing Military Academy's Information Warfare and Command Department's Military Theory Teaching and Research Office, and Major Yang Zhen, a lecturer at the same office, noted that a sovereign state's political system, economic potential, and strategic objectives will be the primary targets attacked in any war against an informatized society. The authors advocated that it is necessary to "defeat the superior with the inferior" and "fight in a way different from how the adversary acts," once again referencing stratagems to buttress their arguments and activities.[28] They espoused that in peacetime, the organized integration of military and economic effects must be achieved; and that in People's War under informatized conditions, both financial and trade warfare must be carried out.[29] Such writings can be interpreted to mean that at least some military officers consider that China is currently at war on the Internet.

In another 2009 *China Military Science* article, Colonel Long Fangcheng and Senior Colonel Li Decai analyzed the role of soft power and its impact on what the Chinese term "comprehensive national power." Somewhat arrogantly, the authors appear to believe that hacker attacks will not lead to any type of severe repercussions from the state under attack. Perhaps this conclusion is based on the current weak responses of nations.

Regarding the use of soft power as an economic tool, the authors suggest:

> In informatized wars, because various types of economic and social activities are based on computers, information, and the Internet to a large extent, social economic life and political life will more heav-

> ily depend on various types of information systems. Information and information systems are weapons…. Paralyzing the enemy country's economy, causing social turmoil to the enemy country, imposing the will of war on the opponent does not lead to large-scale engagements in a traditional sense, and can be effected in a form of soft attacks through network attacks, hacker invasions, and large-scale media warfare, psychological warfare, and legal warfare through news media. Thus the boundary between the state of peace and the state of war will become fuzzy.[30]

Fangcheng and Decai appear to be making the mistaken assumption that an attack on another nation's economy will not lead to any large-scale response. This is dangerous thinking on the part of the Chinese. There is a threshold at which America and other nations will rapidly respond.

An example of a civilian source that emphasizes economic and digital issues is the Chinese book *Internet Wars*. It also focused on the Internet confrontation in general. The book has 18 chapters. Several chapters draw the reader's attention immediately. They are: "The Inevitable Internet War;" "Battles for Internet Control;" "Offensive and Defensive Internet Wars;" "The Internet Will Determine Victory in Future Wars;" "Dangerous Virtual Reality;" and "Financial Wars in the Internet World."[31] The latter should be of particular interest to US analysts.

Dr. Joel Brenner, who worked for the Director of National Intelligence from February 2007 to January 2009, has called China's economic espionage against the United States a national security risk.[32] The United States is, however, initiating actions to confront this risk. In April 2009, the Office of the Secretary of Defense hosted an information warfare simulation focusing on financial attacks on the US economy and the consequences of manipulating financial markets. China, according to one account, proved to be the "savviest economic warrior." Financial specialist Paul Bracken, one of the participants, was worried over the possibility that China might incrementally sell dollars in an attempt to increase economic uncertainty in the United States.[33]

Meanwhile, evidence continues to grow from a number of sources regarding China's economic superiority. Chinese military experts Qiao Liang and Wang Xiangsui, authors of the highly popular and controversial work *Unrestricted Warfare*, have written in another book that the control of the world economic sector has become a goal for the Chinese. They noted that "war with the objective of expanding territory has already basically withdrawn from the state of history, and even war with the objective of fighting for natural resources is now giving way to war with the objective of controlling the flow of financial capital."[34]

People engaged in the world of business activities agree on one thing, the Chinese are excellent at espionage. Most businesspersons readily understand that their Blackberrys, laptops, and cell phone are all compromised once they enter the mainland of China. They also come to expect the bugging of their cars, hotel rooms, and casual conversations. Businessmen feel neutered entering negotiations with the Chinese. Many have noted that it seems as if the Chinese knew every proposal they were going to make and had responses in hand.

China is not overly concerned with privacy issues as we are in the United States. In fact, the state has the preponderance of control over individual cyber rights. This permits the Chinese government to act freely regarding the management of information or its monitoring. The Chinese can establish their own rules for anything they claim to own. This translates into myriad trade restrictions and tariffs, not to mention the undervaluing of the yuan. Outside agencies and customers complain that doing business with China means putting up with their insistence on controlling such activities and actions as foreign encryption protocols companies use to protect sensitive data. Certifications to do business on the mainland are held up until companies comply with Chinese demands, according to Oded Shenkar, a business management professor at the Ohio State University.[35] A 2009 report from the European Union's Chamber of Commerce in China noted that China integrated requirements guaranteeing protectionism into various standardization policies, required for the subjective enforcement of environmental rules favoring Chinese firms. Such policies make it much easier to commit the theft of intellectual property.[36]

The Chinese utilize any number of espionage tools and establish the rules and regulations that stifle attempts by foreign business to participate as an equal in the Chinese market. This is how the Chinese play the game.

Conclusions

The Chinese probes of the world's cyber domains have not ceased. Recently, Canadian researchers uncovered a massive Chinese espionage campaign targeting India. In their report, *Shadow Network*, they outlined the massive campaign emanating from Chengdu, China that harvested a huge quantity of data from India's military and commercial files.

China's activities against Google and India (and their reconnaissance activities in general) portend a much broader pattern, a long-term strategy to hold military and economic assets of various nations hostage. There are a number of Chinese books that support this supposition. Gaining the high ground in international digital competition is becoming a national objective

for the Chinese. China's previous activities certainly afford them a political advantage in any future conflict.

The espionage threat emanating from China is real; and the United States needs to focus on protecting military and economic Internet capabilities if it is to be successful against China's digital reconnaissance effort. Particular focus should be placed on protecting the US military's supply and logistics information, along with financial programs and data. (For example, how might China utilize acquisition of US bonds; or how might Chinese laws and regulations potentially thwart US government and business initiatives?) The challenges for the United States are great, as are the opportunities for China to inflict substantial damage via digital means. The continuing menace of these Chinese electrons remains a subject of conjecture (what is their intent?) that should keep analysts busy throughout the coming years.

NOTES

1. John Markoff, "Cyberattack on Google Said to Hit Password System," *The New York Times*, 19 April 2010, http://www.nytimes.com/2010/04/20/technology/20google.html?_r=1&ref=john_markoff, A1.
2. Josh Rogin, "The Top 10 Chinese Cyber Attacks (that We Know of)," *The Cable*, 22 January 2010, http://thecable.foreignpolicy.com/posts/2010/01/22/the_top_10_chinese_cyber_attacks_that_we_know_of.
3. Kim Zetter, "Google Hackers Targeted Source Code of More than 30 Companies," *Threat Level*, 13 January 2010, http://www.wired.com/threatlevel/2010/01/google-hack-attack.
4. Jessica Guynn, "Chinese Hackers Pose a Growing Threat to U.S. Firms," *The Los Angeles Times*, 15 January 2010, http://articles.latimes.com/2010/jan/15/business/la-fi-google-china15-2010jan15.
5. Ibid.
6. Ibid.
7. Kelly Jackson Higgins, "More Victims of Chinese Hacking Attacks Come Forward," *DarkReading*, 14 January 2010, http://www.darkreading.com/security/attacks/showArticle.jhtml?articleID=222301032.
8. Bryan Krekel, *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation* (Washington: US-China Economic and Security Review Commission, 9 October 2009), 59-63.
9. Ibid.
10. John Markoff and David Barboza, "Two China Schools Said to Be Tied to Online Attacks," *The New York Times*, 18 February 2010, A1, http://www.nytimes.com/2010/02/19/technology/19china.html?emc=eta1nyt.com.
11. Ibid.
12. Ibid.
13. David Barboza, "Hacking Inquiry Puts China's Elite in New Light," *The New York Times*, 22 February 2010, http://www.nytimes.com/2010/02/22/technology/22cyber.html?ref=technology, B1.
14. Ibid.
15. Markoff and Barboza.
16. Ibid.
17. Jon Swartz, "Google Delays Launch of Two Phones in China," USA Today.com, 20 January 2010, B3.
18. Paul McDougall, "China Defends Great Firewall," Information Week.com, 22 January 2010, http://www.informationweek.com/news/government/policy/showArticle.jhtml?articleID=222400246.

19. Thomas Claburn, "Other Targets in Google Cyber Attack Surface," Information Week.com, 15 January 2010, http://www.informationweek.com/news/security/vulnerabilities/showArticle.jhtml?articleID=222301222.

20. Zhang, "Report Says Google to Leave China in April," Chinadaily.com.cn, 20 March 2010, http://english.cri.cn/6909/2010/03/20/53s558001.htm.

21. Li Xiaokun, "Defense Ministry Denies Cyber Attack Support," China Daily Online, in English, 25 February 2010, http://www.chinadaily.com.cn/china/2010-02/25/content_9502911.htm.

22. Jane Macartney, "China Rejects Claims It is behind Cyber Attacks," *The Times*, 11 March 2010, http://technology.timesonline.co.uk/tol/news/tech_and_web/article7056277.ece.

23. Larry Dignan, "China to Google: Censor or 'Pay the Consequences,'" *ZDNet*, 12 March 2010, http://www.zdnet.com/blog/btl/china-to-google-censor-or-pay-the-consequences/31837.

24. "China's Instructions on Reporting on Google," *The Washington Post*, 25 March 2010, A21.

25. David Berlind, "Is the US Afraid to Admit that China Declared War on It?" *Information Week Government Blogs*, 22 January 2010.

26. "Report: Foreign Attacks on US Grid Increasing," *OnDeadline*, 8 April 2009, http://content.usatoday.com/communities/ondeadline/post/2009/04/65244839/1; 2007 Report to Congress of the U.S.-China Economic and Security Review Commission (Washington: US-China Economic and Security Review Commission, 1 June 2007).

27. Ibid., 12.

28. Wang Wei and Yang Zhen, "Recent Development in the Study of the Thought of People's War under Informatized Conditions," China Military Science, 2d iss. 2009, pp. unknown at time of printing.

29. Ibid.

30. Long Fangcheng and Li Decai, "On the Relationship of Military Soft Power to Comprehensive National Power and State Soft Power," China Military Science, 5th iss. 2009, 120-29.

31. Dong Niao, Internet Wars (Bejing: Jiuzhou Press, 2009), 3-7.

32. Shane Harris, "China's Cyber-Militia," *National Journal*, 31 May 2008, http://www.nationaljournal.com/njmagazine/print_friendly.php?ID=cs_20080531_6948.

33. Eamon Javers, "Pentagon Preps for Economic Warfare," Politico.com, 9 April 2009, http://dyn.politico.com/printstory.cfm?uuid=88593103-18FE-70B2-A835D1F6D5DC8F3A.

34. Qiao Liang and Wang Xiangsui, "Fully Calculating the Costs and Profits of War," in On the Chinese Revolution in Military Affairs, ed. Shen Weiguang (Beijing: New China Press, 2004), 105-12.

35. Byron Acohido, Calum MacLeod, and Kathy Chu, "Google Clash Highlights How China Does Business," *USA Today*, 25 January 2010, B2.

36. Ibid.