Journal of Strategic Security

Volume 4
Number 2 *Volume 4, No. 2, Summer 2011: Strategic Security in the Cyber Age*

Article 2

China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence

Magnus Hjortdal
CHINA-SEC, Centre for Military Studies, University of Copenhagen, magnushjortdal@hotmail.com

pp. 1-24

Recommended Citation
Hjortdal, Magnus. "China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence." *Journal of Strategic Security* 4, no. 2 (2011): : 1-24.
DOI: http://dx.doi.org/10.5038/1944-0472.4.2.1
Available at: http://scholarcommons.usf.edu/jss/vol4/iss2/2

China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence

Author Biography

Magnus Hjortdal is a researcher associated with CHINA-SEC, Centre for Military Studies at the University of Copenhagen. He holds an M.Sc. in Political Science from the University of Copenhagen and is owner of MH International Relations, which advises private and public institutions. Former Research Fellow at the Royal Danish Defense College, where he drew assessments and advised Danish authorities. Frequently featured in Danish television, radio, and print media. Expertise: China; East Asia; the U.S.; foreign, defense, and security policy; cyber warfare; intelligence; and espionage.

Abstract

This article presents three reasons for states to use cyber warfare and shows that cyberspace is—and will continue to be—a decisive element in China's strategy to ascend in the international system. The three reasons are: deterrence through infiltration of critical infrastructure; militarytechnological espionage to gain military knowledge; and industrial espionage to gain economic advantage. China has a greater interest in using cyberspace offensively than other actors, such as the United States, since it has more to gain from spying on and deterring the United States than the other way around. The article also documents China's progress in cyber warfare and shows how it works as an extension of its traditional strategic thinking and the current debate within the country. Several examples of cyber attacks traceable to China are also presented. This includes cyber intrusions on a nuclear arms laboratory, attacks on defense ministries (including the Joint Strike Fighter and an airbase) and the U.S. electric grid, as well as the current Google affair, which has proved to be a small part of a broader attack that also targeted the U.S. Government. There are, however, certain constraints that qualify the image of China as an aggressive actor in cyberspace. Some believe that China itself is the victim of just as many attacks from other states. Furthermore, certain actors in the United States and the West have an interest in overestimating China's capabilities in cyberspace in order to maintain their budgets.

Journal of Strategic Security
Volume IV Issue 2 2011, pp. 1-24
DOI: 10.5038/1944-0472.4.2.1

Published Quarterly by Henley-Putnam University Press
with support from the University of South Florida Libraries

China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence

Magnus Hjortdal
CHINA-SEC, Centre for Military Studies, University of Copenhagen
magnushjortdal@hotmail.com

Abstract

This article presents three reasons for states to use cyber warfare and shows that cyberspace is—and will continue to be—a decisive element in China's strategy to ascend in the international system. The three reasons are: deterrence through infiltration of critical infrastructure; military-technological espionage to gain military knowledge; and industrial espionage to gain economic advantage. China has a greater interest in using cyberspace offensively than other actors, such as the United States, since it has more to gain from spying on and deterring the United States than the other way around. The article also documents China's progress in cyber warfare and shows how it works as an extension of its traditional strategic thinking and the current debate within the country. Several examples of cyber attacks traceable to China are also presented. This includes cyber intrusions on a nuclear arms laboratory, attacks on defense ministries (including the Joint Strike Fighter and an airbase) and the U.S. electric grid, as well as the current Google affair, which has proved to be a small part of a broader attack that also targeted the U.S. Government. There are, however, certain constraints that qualify the image of China as an aggressive actor in cyberspace. Some believe that China itself is the victim of just as many attacks from other states. Furthermore, certain actors in the United States and the West have an interest in overestimating China's capabilities in cyberspace in order to maintain their budgets.

Journal of Strategic Security

Introduction

"In today's information age, the People's Republic of China has replaced and even improved upon KGB methods of industrial espionage to the point that the People's Republic of China now presents one of the most capable threats to U.S. technology leadership and by extension its national security."[1]

—Dan Verton, Cyber Warfare Expert

Recently, China has been labeled a hacker state by mainstream media; therefore, the purpose of this article is to contribute to the debate by providing information about China's true capabilities in cyberspace. The article further aims to explain and explore why China maintains and utilizes an aggressive cyber warfare posture; namely, cyberspace is an important dimension in present Chinese foreign and security politics. Examples are then provided that seek to explain why the United States feels threatened.

China's capabilities in cyberspace are analyzed through a strategic lens, and it is argued that the development of China's cyberspace capability can ensure its ascent to a future superpower status. The article concludes that China is most likely behind many of the attacks presented in mainstream media. Furthermore, China deliberately uses its cyber warfare capabilities to deter the United States. This strategy may ensure eventual strategic parity with the United States in technological and military prowess.

Cyber Warfare

Cyberspace is essential in modern warfare at the operational level, where soldiers are increasingly dependent on cyberspace; and at the strategic level, where a state's weaknesses and strengths in cyberspace can be used to deter and affect the strategic balance of power.

What is cyber warfare? The highly regarded London-based International Institute for Strategic Studies (IISS) generally considers cyber warfare as an intellectually underdeveloped field very similar to the lack of research on the dynamics of nuclear weapons in the 1950s. IISS Director-General and Chief Executive John Chipman recently said that "future state-on-state conflict may be characterized by the use of so-called asymmetric techniques. Chief among these may be the use of cyber-warfare."[2]

http://scholarcommons.usf.edu/jss/vol4/iss2/2
DOI: http://dx.doi.org/10.5038/1944-0472.4.2.1

The dynamics of the cyberspace realm mean that it is easier to attack than to defend.[3] According to the 2010 *U.S. Quadrennial Defense Review*, "the speed of cyber attacks and the anonymity of cyberspace greatly favors the offence. This advantage is growing as hacker tools become cheaper and easier to employ by adversaries whose skills are growing in sophistication."[4]

There are three reasons for states to maintain and utilize an aggressive cyber capability:[5]

1. to deter other states by infiltrating their critical infrastructure;[6]

2. to gain increased knowledge through espionage in cyberspace, which makes it possible for states to advance more quickly in their military development;[7]

3. to make economic gains where technological progress has been achieved—for example, through industrial espionage.[8] This can be carried out outside official institutions.

States may also need advanced cyber warfare capabilities for a further reason—namely, in order to be able to attack and paralyze an adversary's military capacity or the adversary's ability to control its own forces.[9] As this fourth reason will only become apparent during times of conflict and actual warfare, it will not be considered further in this article, since there are no examples of it regarding present relations between China and the United States.

An analysis of Chinese state capabilities in cyberspace is an extremely relevant object of study since China gains greater advantage from possessing offensive capabilities in cyberspace than most other state actors. It must be emphasized, however, that the purpose of this article is not to present China as the only bad kid on the block that is breaking the rules of good behavior.

The West and the United States, for example, may also be expected to act similarly to what China is accused of doing.[10] However, an analysis of American capabilities is not the topic here since the United States does not have as much to gain relative to China by developing an aggressive cyber capability. This can be seen in light of the three reasons previously cited for which states seek to maintain and utilize such a capability. First, the United States does not need to deter other states via cyberspace, since it manages just fine militarily. Secondly, the reality today is that since U.S. military technology is second to none, intensive espionage to gain knowl-

edge about other states' military technology is not necessary. As for the third reason regarding economic advantage, industrial espionage has less significance for the United States since industrial-technological levels in the United States are among the most advanced in the world.

China, on the other hand, with regard to the first reason, has an interest in avoiding exposure to political and military pressure from the West and the United States. Secondly, China also has an interest in accelerating its military development since it is still far behind the West in general. And finally, with regard to the third reason, China's general technological level is also behind that of the United States, which gives it an increased incentive for industrial espionage in order to achieve economic advantage.

It is thus especially pertinent to examine China's capability in cyberspace, but we must nonetheless remember that other state actors use the same techniques. The difference is that the incentives to use cyberspace offensively are fewer for the West and the United States by comparison.

Cyber capabilities are not a subject that states discuss openly, since it is rarely beneficial for a state to publicize that it is spying on another state or that it is causing another state's networks to close down. Much is written about the vital importance of possessing a cyber capability,[11] and while states do not directly announce their own offensive capabilities in cyberspace, this does not prevent them from discussing and analyzing other states' capabilities and options in this area.[12] The uncertainty about the actual sophistication of China's capabilities can deter the United States and other states further, since, according to classical military logic, states must be prepared for the worst when they do not know the actual strength of their potential rivals.

By acting aggressively, states can increase the risk of accusations that they are carrying out cyber attacks, which paradoxically can benefit a country like China. This is because the deterrent aspect of possessing advanced cyber capabilities might not otherwise be detected or widely known. In other words, if North Korea were the only state in the world that knew it had nuclear arms and the rest of the world was convinced that this was *not* the case, then the deterrent element of North Korea's nuclear weapons program would not exist. The strategy of deterrence is thus two-sided and, as such, contradictory—a balancing act is needed between hiding the maximum level of capability on the one hand, and communicating and proving that the capability exists on a sufficiently high level to deter other states on the other.

http://scholarcommons.usf.edu/jss/vol4/iss2/2
DOI: http://dx.doi.org/10.5038/1944-0472.4.2.1

China's Thinking and Capabilities in Cyberspace

China's military strategy mentions cyber capabilities as an area that the People's Liberation Army (PLA) should invest in and use on a large scale.[13] The U.S. Secretary of Defense, Robert Gates, has also declared that China's development in the cyber area increasingly concerns him,[14] and that there has been a decade-long trend of cyber attacks emanating from China.[15]

Virtually all digital and electronic military systems can be attacked via cyberspace. Therefore, it is essential for a state to develop capabilities in this area if it wishes to challenge the present American hegemony. The interesting question then is whether China is developing capabilities in cyberspace in order to deter the United States.[16]

Box 1: Concepts of cyber warfare

The general NATO term is *Computer Network Operations (CNO)*.

Under CNO three elements can be identified:[17]

1. Computer-Network Exploitation (CNE), which covers attempts to gather information about a system to use for later attacks

2. Computer-Network Attack (CNA), which covers attempts to attack systems

3. Computer-Network Defense (CND), which refers to one's own defense against an attack

The connection among the three is that effective CNA cannot be carried out without also having CNE and CND and vice versa.

In China, CNO and outer space capabilities are covered by the same term, *informationization*, whereas CNO covers the cyberspace part of the Chinese term.[18]

China's military strategists describe cyber capabilities as a powerful *asymmetric* opportunity in a *deterrence* strategy.[19] Analysts consider that an "important theme in Chinese writings on computer-network operations (CNO) is the use of computer-network attack (CNA) as the spearpoint of deterrence."[20] CNA increases the enemy's costs to become too great to engage in warfare in the first place, which Chinese analysts judge

to be essential for deterrence.[21] This could, for example, leave China with the potential ability to deter the United States from intervening in a scenario concerning Taiwan. CNO is viewed as a focal point for the People's Liberation Army, but it is not clear how the actual capacity functions or precisely what conditions it works under.[22]

If a state with superpower potential (here China) is to create an opportunity to ascend militarily and politically in the international system, it would require an asymmetric deterrence capability such as that described here.[23]

It is said that the "most significant computer network attack is characterized as a pre-emption weapon to be used under the rubric of the rising Chinese strategy of [...] gaining mastery before the enemy has struck."[24] Therefore, China, like other states seeking a similar capacity, has recruited massively within the hacker milieu inside China.[25] Increasing resources in the PLA are being allocated to develop assets in relation to cyberspace.[26] The improvements are visible: The PLA has established "*information warfare*" capabilities,[27] with a special focus on cyber warfare that, according to their doctrine, can be used in peacetime.[28] Strategists from the PLA advocate the use of virus and hacker attacks that can paralyze and surprise its enemies.[29]

Aggressive and Widespread Cyber Attacks from China and the International Response

China's use of asymmetric capabilities, especially cyber warfare, could pose a serious threat to the American economy.[30] Research and development in cyber espionage figure prominently in the 12th Five-Year Plan (2011–2015) that is being drafted by both the Chinese central government and the PLA.[31]

Analysts say that China could well have the most extensive and aggressive cyber warfare capability in the world, and that this is being driven by China's desire for "global-power status."[32] These observations do not come out of the blue, but are a consequence of the fact that authoritative Chinese writings on the subject present cyber warfare as an obvious asymmetric instrument for balancing overwhelming (mainly U.S.) power, especially in case of open conflict, but also as a deterrent.[33]

http://scholarcommons.usf.edu/jss/vol4/iss2/2
DOI: http://dx.doi.org/10.5038/1944-0472.4.2.1

In general, China is very active on the cyber scene.[34] A high Chinese level of capability is indicated when, for example, it has allegedly infiltrated computers in 103 countries in order to keep an eye on exiled Tibetans' struggle for a free Tibet.[35]

Box 2: Statements about China's cyber capabilities

"Critical U.S. infrastructure is vulnerable to malicious cyber activity. Chinese military doctrine calls for exploiting these vulnerabilities in the case of a conflict."

The U.S.–China Economic and Security Review Commission 2009[36]

"[The Chinese government] resolutely oppose[s] any crime, including hacking, that destroys the Internet or computer network [...]; some people overseas with Cold War mentality are indulged in fabricating the sheer lies of the so-called cyberspies in China."

Wang Baodung, spokesman for the Chinese Embassy in Washington, April 2009[37]

While American security experts call the U.S. defense against cyber attacks "embarrassing" and state that it "has effectively run out of steam,"[38] China is allocating many resources to its cyber program.[39] Nonetheless, the director of the U.S. Department of Homeland Security has stated that cyber attacks can be compared to the attacks on September 11, 2001, and that "[w]e take threats to the cyber world as seriously as we take threats from the material world."[40] Indeed, a 2007 cyber attack on an American nuclear arms laboratory confirms the need to take the threats from cyberspace very seriously. It is not known with any certainty how much data was downloaded,[41] but the attack could be traced to China, and all the indications are that it was carried out by state organizations. At worst, it might have resulted in the transfer of American nuclear weapons technology.

In the United Kingdom (UK), a 14-page document from MI5 called "The Threat from Chinese Espionage," drawn up in 2008, has now made it into public spheres. The restricted report said that "[a]ny UK company might be at risk if it holds information which would benefit the Chinese."[42] Furthermore, the report describes how China's cyber warfare campaign had

targeted British defense, energy, communications and manufacturing companies, as well as public relations and international law firms, some of them being a vital part of the British critical infrastructure.[43]

In 2009, the British Joint Intelligence Committee, which coordinates work between the two intelligence services, MI5 and MI6, warned that China's cyber espionage is becoming very sophisticated and mature in its approach. It was described how this could enable China to shut down critical services, including power, food, and water supplies.[44] This is not the first time that China has been accused of aggressive cyber operations by the British. The head of the UK's domestic intelligence service, MI5, stated in December 2007 that it was under (cyber) attack by "Chinese state organizations."[45]

China's offensive cyber capabilities are identified in numerous additional UK reports from analysts and defense ministries. They describe a Chinese military exercise as early as 2005 directly aimed at practicing hacking into enemy networks.[46] The vice-chairman of the U.S. Joints Chiefs of Staff, General James Cartwright, has said that a full-scale Chinese cyber attack potentially has the same effect as weapons of mass destruction.[47] This has triggered a lively discussion on whether the same dynamics created by nuclear weapons can apply in a new context.[48, 49] Furthermore, one western expert says, with clear reference to Chinese cyber warriors: "Let's say an emerging superpower would dedicate 20,000, 30,000, 40,000 people and then unleash that force at some point, I would say we would not be ready."[50]

The Deterrence Effect on the United States: Electricity Grids and an Airbase

Cyber capabilities have a real deterrent effect when a state shows its capabilities to the world. This happened when the United States became aware that its electricity network had been hacked into in 2009 and that parts of the network allegedly could be shut down whenever the hacker wished to do so.[51] Other sources, even though a little more skeptical about the scope of such intrusions, indicate that although these foreign intruders did not cause immediate damage, they left behind software programs that could be used in the future to disrupt this critical infrastructure.[52] This attack was traced to China, and the chief of counterintelligence in the United States at the time stated that "[w]e have seen Chinese network operations inside certain of our electricity grids."[53] The fact that Americans were not able to protect their electricity network is one critical aspect, but another is that this shows that the United States could have a serious problem in

http://scholarcommons.usf.edu/jss/vol4/iss2/2
DOI: http://dx.doi.org/10.5038/1944-0472.4.2.1

meeting the challenge of an ambitious Chinese cyber program.[54] U.S. security experts have previously expressed their concerns. After the April 2007 cyber attacks on Estonia, following a surge of nationalism from Russia that caused a severe breakdown and paralyzed the heavily IT-based Estonian infrastructure, Pentagon cyber security expert Sami Saydjari told the U.S. Congress that "a similar mass cyber attack could leave the United States without power for six months—sufficient time to allow China to occupy Taiwan, or Russia to 'liberate' Georgia."[55] Such statements pinpoint the vulnerability of U.S. critical infrastructure. At present, the United States is also behind China with regard to the training of engineers who can be used in cyber-related functions.[56]

In addition, an American airbase was forced to shut off its network and stop takeoffs and landings for a time, due to a massive virus attack traced to China.[57] We can only guess about the exact state of security in other western countries, but the level is hardly much higher than in the United States. Recent developments indicate that the level in NATO and the EU is even more vulnerable to cyber attacks because each member state is required to have its own cyber defense.[58]

More Cyber Attacks: Joint Strike Fighter, Pentagon, and Merkel

In 2009, there was a forced electronic entry into the Joint Strike Fighter program and large amounts of data were copied.[59] According to present and former employees at the Pentagon, the attack can be traced to China.[60] This *could* mean that it would be easy for China to defend itself against the aircraft (which many western countries expect to acquire) and, assuming the attackers have acquired enough data, they may even be able to copy parts of it.[61] The American chief of counterintelligence has been reported as saying that "our networks are being mapped" with reference to American flight traffic control, and also as having warned about a situation in which "a fighter pilot can't trust his radar."[62]

The Pentagon has already had a "computer security incident," apparently involving the malevolent use of Universal Serial Bus (USB) memory sticks, after which these sticks were banned.[63] China is the world's largest producer of USB memory sticks,[64] and certain observers speak informally about the possibilities a state would have if it could program all the USB memory sticks produced in the country so that information about the content of the computers using them could be sent back to a center at home. This is, of course, a paranoid thought experiment, but it clearly illustrates the fear and seriousness that cyber warfare and hacking inspire. On the

other hand, no reports suggest that the Pentagon's internal communications system has been hacked into, so at present it seems that no U.S. vital wartime communications have been compromised.

The office of the German chancellor, Angela Merkel, has also been hacked into and very sensitive data copied. The attack was later traced back to China.[65] The fact that it was possible to break into Merkel's computer has great implications for the seriousness of China's capabilities in cyberspace. To underline the German worries of Chinese cyber attacks, German counterintelligence agent Walter Opfermann has said that China is stealing industrial secrets in great numbers and also is capable of "sabotaging whole chunks of infrastructure," such as the German power grid. He concludes that "[t]his poses a danger not just for Germany but for critical infrastructure worldwide."[66]

Google Was Just a Little Part of a Larger Attack

In connection with a massive hacker attack against Google's email customer accounts in December 2009,[67] it has since become clear that the attacks (which caused Google to withdraw temporarily from its cooperation on censorship) formed just a small part of a larger cyber attack against at least 34 American companies and institutions with links to the U.S. administration, including suppliers to the Pentagon and even some members of the U.S. Congress.[68] The Google affair attracted great media attention to an area of great concern for the United States. Reports have linked two Chinese educational institutions to the attacks on Google: Lanxiang Vocational School based in Jinan, Shandong province; and Shanghai Jiaotong University.[69] In a point of departure from cyber deterrence, the Google affair was likely a Chinese attempt to spy on what Beijing labels "separatists," and was likely not a part of any strategic deterrence strategy.[70]

Analysts from the U.S. Government, including experts from the National Security Agency (NSA), remain certain that a Chinese security consultant in his thirties made the program that was used to launch the attacks on Google and more than 30 other companies.[71] According to the sources, "[t]he spyware creator is a freelancer and did not launch the attack, but Beijing officials had 'special access' to his programming."[72] In a report identifying the origin of the attacks in December 2009, experts from VeriSign Defence stated without reservation that the Chinese Government was behind them.[73] At the same time, a classified FBI report was leaked, claiming that China had developed a "cyber army" comprising 30,000 military cyber spies plus 150,000 spies hired from the private sector.[74]

http://scholarcommons.usf.edu/jss/vol4/iss2/2
DOI: http://dx.doi.org/10.5038/1944-0472.4.2.1

The report states that their mission was to steal American military and technological secrets,[75] something also described by the leading officer of the U.S. Pacific Command, Admiral Robert Willard.[76]

Box 3: Who is behind China's cyber warfare?[77]

Public part of cyber warfare

The public part of cyber warfare in China is directed by the PLA General Staff, 4th Department (Electronic Countermeasures and Radar). CND and CNE are delegated to the PLA General Staff, 3rd Department (Signals Intelligence and Technical), that roughly is equivalent to the U.S. National Security Agency. "Training in CNO occurs across all People's Liberation Army service branches, from command to company level, and is considered a core competence of all combat units. Field exercises include joint operations in 'complex electromagnetic environments,' and sources indicate the existence of a permanent 'informationized Blue Force' regiment, drilled in foreign Information Warfare tactics."

Military-civilian blurring

Examples of cooperation between private hackers and the PLA do occur. Hackers have even publicly referred to their incorporation into PLA operations in a 2005 message on the hacker community called the Honker Union of China. The message stated that the hackers have "government-approved network technology security units."

Further indication of the formal and informal cooperation between the military and civilian parts are seen in PLA's sponsorship of numerous universities and institutes supporting research and development in information warfare. "These include the Science and Engineering University in Hefei, the Information Engineering University in Zhengzhou, the National University of Defense Technology in Changsha, and the Communications Command Academy in Wuhan."

The spokesperson from the Chinese Ministry of National Defense has said that, "[l]inking the cyber hacking with the Chinese Government and military is baseless, highly irresponsible, and hype with ulterior motives."[78] Nevertheless, it might not be biased or irresponsible to suspect the Chinese state, as most experts point to Beijing being behind the Google attacks.[79] Dan Blum, a leading analyst from IT consultancy Burton Group, said the preponderance of evidence pointed to Chinese involve-

ment. "Myself, and a lot of people, are well past 99% sure."[80] Leading U.S. scholar Larry Wortzel is also quite certain that the Chinese Government was involved in the recent cyber attacks, as well as several in the past.[81]

One of the most recognized experts in this area, James A. Lewis, produced this concise analysis of the attacks: "This is a big espionage program aimed at getting high-tech information and politically sensitive information—the high-tech information to jump-start China's economy and the political information to ensure the survival of the regime [...]. This is what China's leadership is after. This reflects China's national priorities."[82] Besides that, Mike McConnell, who is former Director of the NSA and Director of National Intelligence (DNI), has recently said that "The United States is fighting a cyber-war today, and we're losing."[83]

Constraints

How capable and effective is Chinese cyber warfare capability?

1. *Who actually attacks whom?* China's own network appears to be unprotected, and other countries can launch attacks through China, which makes it appear the primary suspect.[84] IT expert Steve Armstrong furthermore states that "[i]t's too easy to blame China [...] In fact, legitimate countries are bouncing their attacks through China. It's very easy to do, so why not? [...] My evil opinion is that some western governments are already doing this."[85]

2. *Actors in the United States have an interest in exaggerating China's capabilities*. In order to justify their existence and obtain increased budgets, several actors in the United States may have an interest in presenting China as a threat to U.S. security. The Pentagon, specific politicians, and the intelligence services are often accused of acting as they did during the Cold War, thus contributing to conflict-like relations between China and the United States.[86]

3. *China proposes global cooperation against hacking*.[87] This might sound like a sound proposal, but as described throughout this article, certain states have much to gain by carrying out cyber attacks, which makes cooperation difficult. Besides, it is extremely hard to see how such cooperation could be enforced and by whom.

http://scholarcommons.usf.edu/jss/vol4/iss2/2
DOI: http://dx.doi.org/10.5038/1944-0472.4.2.1

4. It is also possible to imagine that *in China, CNO has an anarchic leadership structure,* meaning that the central leadership cannot control who carries out attacks. Some American reports indicate this very fact.[88] Critical voices say, however, that this is just due to the way the Chinese use hackers from outside the military and the government to carry out attacks.[89]

5. *China denies having any military hackers in the country*.[90] Other countries would most likely deny the same, but to what extent soldiers in the PLA with high-level IT knowledge are being used to carry out cyber attacks is another question. Based on the references cited in this article, it is likely that the PLA uses hackers for espionage.

6. Some think that focusing on China's capabilities does not deal with the fact that *Beijing itself is very dependent on cyberspace* for military and civilian purposes. This means that at the same time as China is developing cyber warfare techniques, its own vulnerability is often overlooked.[91] I would argue that China can still deter the U.S., even though the U.S. is more powerful in all spheres. This is due to the dynamics of the asymmetrical techniques that China pursues, e.g., in cyberspace, which are changing the dynamics of the balance of power that we knew during the Cold War.

In spite of the constraints above, an understanding of the importance of cyber warfare is found in the PLA's strategic thinking.[92] This form of asymmetric strategy has been debated internally for a long time,[93] and a book that attracted much attention, *Unrestricted Warfare*, written by two Chinese colonels, states that "[i]n the information age, the influence exerted by a nuclear bomb is perhaps less than the influence exerted by a hacker."[94]

Conclusion

The evidence in this article has contextualized the elements of cyber warfare capabilities. On the basis of three reasons put forward for states to maintain and utilize the cyber domain aggressively, an analysis was made of China's cyber warfare capabilities. The analysis has shown that China is likely to have conducted several cyber attacks in the past and present, and probably will continue with that strategy in the future, as this is of great importance for its economy, military, and deterrence of the United States.

Implications: China as Cyberpower and Superpower

In the foreword to the Australian Defense White Paper entitled *Defending Australia in the Asia Pacific Century: Force 2030*, on the country's future defense policy, the Australian defense minister, Joel Fitzgibbon, writes:

> "[C]yber warfare has emerged as a serious threat to critical infrastructure [and] the biggest changes to our outlook over the period have been the rise of China [...] [T]he beginning of the end of the so-called unipolar moment; the almost two-decade-long period in which the pre-eminence of our principal ally, the United States, was without question."[95]

The unipolar moment during which the United States could ensure all its allies' security is undergoing change, and China's capabilities for cyber warfare are an important element in this change.

In order to meet this challenge, the United States has now launched a new "Cyber Command" and appointed a "Cyber Czar" to coordinate national preparedness.[96] It should also not be forgotten that the United States is doing a lot on both defensive and offensive cyber network operations.[97] In the dynamics of CNO, where it is far more difficult to defend than to attack,[98] it will be extremely difficult for the United States to counter China's capabilities in this area. America will continue to give its cyber capabilities a high priority, but the cumulative deterrence effect may not be known until the future, if at all.[99] But along with such efforts, the Chinese will also try to avoid a situation in which their deterrent capabilities become neutralized.

In sum, ascending states have much to gain from an offensive and aggressive cyber capability, primarily because of the fact that it is difficult to prove directly who is behind such attacks. Thus, there is a high probability that the Chinese build-up in the cyber area will continue. China's cyber deterrence capability in the longer term will make it possible for further Chinese expansion in the political-military area so that one day, China may become a *de jure* superpower across economic, technological, and military domains.

Frankly, the Chinese cyber deterrence is a strategically intelligent solution that is quite cheap, compared to a full-scale conventional military, and it is capable of effectively deterring the United States from a large-scale conventional military engagement.

http://scholarcommons.usf.edu/jss/vol4/iss2/2
DOI: http://dx.doi.org/10.5038/1944-0472.4.2.1

About the Author

Magnus Hjortdal is a researcher associated with CHINA-SEC, Centre for Military Studies at the University of Copenhagen. He holds an M.Sc. in Political Science from the University of Copenhagen and is owner of MH International Relations, which advises private and public institutions. Former Research Fellow at the Royal Danish Defense College, where he drew assessments and advised Danish authorities. Frequently featured in Danish television, radio, and print media. Expertise: China; East Asia; the U.S.; foreign, defense, and security policy; cyber warfare; intelligence; and espionage.

Acknowledgments

The author would like to thank Sjoerd J.J. Both, Peter J.B. Gottlieb, Simon Ingemar, Ditte Toefting-Kristiansen, Robert S. Ross, and Larry Wortzel for their helpful comments and suggestions.

References

1 Dan Verton, "The Evolution of Espionage: Beijing's Red Spider Web," *China Brief* 8:15 (2008): 4.

2 International Institute for Strategic Studies (IISS), "The Military Balance 2010, Press Statement," remarks by Dr. John Chipman (February 3, 2010), available at: *http://tinyurl.com/6abm5pn (www.iiss.org/publications/military-balance/the-military-balance-2010/military-balance-2010-press-statement/)*.

3 Dennis C. Blair, *"Annual Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence"* (Washington D.C.: Office of the Director of National Intelligence, 2010), 3. In general, cyber warfare often consists of intertwined defensive, offensive, civil and military components.

4 Department of Defense, *Quadrennial Defense Review Report* (Washington D.C.: U.S. Department of Defense, 2010), 37.

5 In Denmark, the Danish Defence Intelligence Service (Forsvarets Efterretningstjeneste, FE), in its annual risk assessment, writes that "[t]he threat from espionage continues [to come] from certain foreign intelligence services that are interested in Danish Defence, Danish Defence's international involvement, NATO and European security and defence cooperation." In addition, FE states that "espionage continues [to occur] through a broad range of methods, from use of open sources such as the Internet to undercover operations in which they attempt to use other persons to gain information. There are no indications that this intelligence threat will lessen." See Forsvarets Efterretningstjeneste (FE), *Efterretningsmæssig risikovurdering 2009*, August 28, 2009, available at: *http://tinyurl.com/6xtmv68 (fe-ddis.dk/SiteCollectionDocuments/FE/EfterretningsmaessigeRisikovurderinger/risikovurdering2009.pdf)*, 19.

6 Larry Wortzel, "China's Approach to Cyber Operations: Implications for the United States," testimony before the Committee on Foreign Affairs, House of Representatives, Hearing on "The Google Predicament: Transforming U.S. Cyberspace Policy to Advance Democracy, Security, and Trade," March 10, 2010, available at: *http://www.internationalrelations.house.gov/111/wor031010.pdf*, 4–5; Northrop Grumman, *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*, report prepared for The US–China Economic and Security Review Commission (USCC), (McLean, VA: Northrop Grumman Corporation, Information Systems Sector, 2009), 19–20; "War and PC: Cyberwarfare," *Jane's Defence Weekly*, September 19, 2008.

7 Northrop Grumman, *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*, 51–58; Larry Wortzel, "China's Approach to Cyber Operations: Implications for the United States," 2–3; "Breaching protocol—the threat of cyberespionage," *Jane's Intelligence Review*, February 11, 2010, available at: *http://tinyurl.com/3snjmu9 (articles.janes.com/articles/Janes-Intelligence-Review-2010/Breaching-protocol--the-threat-of-cyberespionage.html)*.

8 Northrop Grumman, *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*, 51–58; Larry Wortzel, "China's Approach to Cyber Operations: Implications for the United States," 2–3; "Breaching protocol—the threat of cyberespionage," *Jane's Intelligence Review*.

9 Xu Rongsheng, Chief Scientist at the Cyber Security Lab of the Institute for High Energy Physics of the Chinese Academy of Sciences, told a Chinese news reporter that "Cyber warfare may be carried out in two ways: in wartime, to disrupt and damage the networks of infrastructure facilities, such as power systems, telecommunications systems, and education systems, in a country; or in military engagements, the cyber technology of the military forces can be turned into combat capabilities." Larry Wortzel, "China's Approach to Cyber Operations: Implications for the United States," 6.

10 "Breaching protocol—the threat of cyberespionage," *Jane's Intelligence Review*. Cyber warfare was first put on the public agenda when Estonia was paralyzed for several days during what seemed to be a Russian cyber attack on Estonian critical infrastructure over a heated nationalist debate over Russia's legacy in Estonia; see Gadi Evron, "Battling Botnets and Online Mobs: Estonia's Defense Efforts during the Internet War," *Georgetown Journal of International Affairs*, Winter/Spring (2008): 121, 123–124; "Estonia hit by 'Moscow cyber war,'" *BBC News*, May 17, 2007, available at: *http://news.bbc.co.uk/go/pr/fr/-/2/hi/europe/6665145.stm*; Tony Halpin, "Estonia accuses Russia of 'waging cyber war,'" *Times Online*, May 17, 2007, available at: *http://www.timesonline.co.uk/tol/news/world/europe/article1802959.ece*. Also, during the Georgian war, Russia allegedly conducted several cyber attacks penetrating official Georgian government websites; see Eneken Tikk, Kadri Kaska, Kristel Rünnimeri, Mari Kert, Anna-Maria Talihärm, and Liis Vihul, *Cyber Attacks Against Georgia: Legal Lessons Identified* (Tallinn, Estonia: Cooperative Cyber Defence Centre of Excellence, 2008), available at: *http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf*, 12–13; "Georgia targeted in cyber attack," *AFP*, August 18, 2008, available at: *http://afp.google.com/article/ALeqM5iRuGsssizXAKVgmPqAXOxqB5uHsQ*;

http://scholarcommons.usf.edu/jss/vol4/iss2/2
DOI: http://dx.doi.org/10.5038/1944-0472.4.2.1

Mark Watts, "Cyberattacks became part of Russia–Georgia war," *Computer-Weekly*, August 13, 2008, available at: *http://tinyurl.com/67z4dm (www.computerweekly.com/Articles/2008/08/13/231812/cyberattacks-became-part-of-russia-georgia-war.htm)*.

11 State Council, *China's National Defence in 2008* (Beijing: Information Office of the State Council of the People's Republic of China, Foreign Languages Press, 2009), 8–11.

12 Office of the Secretary of Defence, *Annual Report to Congress: Military Power of the People's Republic of China 2009* (Washington: U.S. Department of Defence, 2009), 17, 24.

13 Chen Zhou, "A Review of China's Military Strategy," *China Armed Forces* 1:1 (2009): 19.

14 Lin Cheng-yi, "China's 2008 Defence White Paper: The view from Taiwan," *China Brief* IX:3 (2009): 14.

15 "Breaching protocol – the threat of cyberespionage," *Jane's Intelligence Review*.

16 It could also be interesting to investigate how other western countries may react to China's capabilities in the cyber area.

17 See James Mulvenon, "PLA Computer Network Operations: Scenarios, Doctrine, Organizations, and Capability," in: Roy Kamphausen, David Lai, and Andrew Scobell (eds.), *Beyond the Strait: PLA Missions Other Than Taiwan* (Carlisle, PA: Strategic Studies Institute, U.S. Army War College, 2009), 257–259.

18 State Council, *China's National Defense in 2008*, 7.

19 James Mulvenon, "PLA Computer Network Operations: Scenarios, Doctrine, Organizations, and Capability," 257.

20 Ibid.

21 Timothy L. Thomas, "Nation-state Cyber Strategies: Examples from China and Russia," in Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (eds.), *Cyberpower and National Security* (Dulles, VA: Potomac Books, Inc. and NDU Press, 2009), 468; James Mulvenon, "PLA Computer Network Operations: Scenarios, Doctrine, Organizations, and Capability," 258.

22 Marc Miller, *PLA Missions Beyond Taiwan*, Colloquium Brief (Carlisle, PA: Strategic Studies Institute, U.S. Army War College, 2008), 3. This is the author's opinion, in spite of an American report that points out concrete locations where China's cyber warfare units are supposed to be located; see U.S.-China Economic and Security Review Commission (USCC), *2009 Report to Congress of the U.S.-China Economic and Security Review Commission* (Washington: U.S. Government Printing Office, 2009), 172–176.

23 Timothy L. Thomas, "Nation-state Cyber Strategies: Examples from China and Russia," 469, 475.

24 James Mulvenon, "PLA Computer Network Operations: Scenarios, Doctrine, Organizations, and Capability," 259.

25 Northrop Grumman, *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*, 7; James Mulvenon, "PLA Computer Network Operations: Scenarios, Doctrine, Organizations, and Capability," 277–278.

26 Marc Miller, *PLA Missions Beyond Taiwan*, 2–3.

27 Information Warfare: in brief, all wars that can be carried out through the use of and against information technology; see Bruce D. Berkowitz, "Wartime in the Information Age," in: John Arquilla and David Ronfeldt (eds.), *In Athena's Camp: Preparing for Conflict in the Information Age* (Santa Monica, CA: RAND Corporation, 1997), 175–177.

28 Tai Ming Cheung, "Dragon on the Horizon: China's Defence Industrial Renaissance," *Journal of Strategic Studies* 32:1 (2009): 29–66.

29 Ibid., 35.

30 U.S.-China Economic and Security Review Commission (USCC), *2009 Report to Congress of the U.S.-China Economic and Security Review Commission* (Washington: U.S. Government Printing Office, 2009), 167–183; Office of the Secretary of Defense, *Annual Report to Congress: Military Power of the People's Republic of China 2009*, 20. Yet, in case of a conflict, other western countries would feel similarly vulnerable.

31 Willy Lam, "Beijing Bones up its Cyber-Warfare Capacity," *China Brief* X:3 (2010): 2–4.

32 Stratfor, "China: Pushing Ahead of the Cyberwarfare Pack," March 2, 2009, available at: *http://tinyurl.com/5u6j4qc (www.stratfor.com/memberships/132785/analysis/20090225_china_pushing_ahead_cyberwarfare_pack).*

33 Qiao Liang and Wang Xiangsui, *Unrestricted Warfare,* Beijing: PLA Literature and Arts Publishing House, 1999, 29, 47, 211–212.

34 Dan Verton, "The Evolution of Espionage: Beijing's Red Spider Web," 5–7.

35 John Markoff, "Vast Spy System Loots Computers in 103 Countries," *New York Times*, March 28, 2009, available at: *http://www.nytimes.com/2009/03/29/technology/29spy.html*.

36 U.S.-China Economic and Security Review Commission (USCC), *2009 Report to Congress of the U.S.-China Economic and Security Review Commission*, 181.

37 Siobhan Gorman, "Electricity Grid in U.S. Penetrated by Spies," *Wall Street Journal*, April 8, 2009, available at: *http://online.wsj.com/article/SB123914805204099085.html*.

38 Maggie Shiels, "US cybersecurity 'embarrassing,'" *BBC News*, April 29, 2009, available at: *http://news.bbc.co.uk/2/hi/technology/8023793.stm*.

39 David E. Sanger, John Markoff, and Thom Shanker, "U.S. Steps up Effort on Digital Defenses," *New York Times*, April 27, 2009, available at: *http://www.nytimes.com/2009/04/28/us/28cyber.html*.

40 Maggie Shiels, "Cyber risk 'equals 9/11 impact,'" *BBC News*, April 8, 2008, available at: *http://news.bbc.co.uk/2/hi/technology/7335930.stm*.

http://scholarcommons.usf.edu/jss/vol4/iss2/2
DOI: http://dx.doi.org/10.5038/1944-0472.4.2.1

41 John Markoff, "Cyber attack on U.S. nuclear arms lab linked to China," *New York Times*, November 9, 2007, available at: *http://tinyurl.com/64q929e (www.nytimes.com/2007/12/09/world/americas/09iht-hack.1.8653712.html)*.

42 David Leppard, "China bugs and burgles Britain," *Times Online*, January 31, 2010, available at: *http://www.timesonline.co.uk/tol/news/uk/crime/article7009749.ece*.

43 Ibid.

44 John F. Burns, "Britain Warned Businesses of Threat of Chinese Spying," *New York Times*, February 1, 2010, available at: *http://www.nytimes.com/2010/02/01/world/europe/01spy.html*.

45 No author, "Spy Chief in Britain accuses China of cyber crime," *New York Times*, December 2, 2007, available at: *http://tinyurl.com/68l8arm (www.nytimes.com/2007/12/02/world/europe/02iht-cyber.1.8557238.html)*.

46 "War and PC: cyberwarfare," *Jane's Defence Weekly*; No author, "Chinese hackers attack British parliament," *South China Morning Post*, September 5, 2007.

47 "War and PC: cyberwarfare," *Jane's Defence Weekly*.

48 Dynamics such as "Mutually Assured Destruction" (MAD) that led to mutual deterrence between the U.S. and the Soviet Union during the Cold War. The Chinese already use a counterpart to MAD in their strategy for outer space capabilities, which they call a "space balance of force;" see Michael Krepon, "China's Military Space Strategy: An Exchange," *Survival*, 50:1 (2008): 174.

49 "U.S. Steps Up Effort on Digital Defenses," *New York Times*; Mike McConnell, "Mike McConnell on how to win the cyber-war we're losing," *Washington Post*, February 28, 2010 available at: *http://tinyurl.com/ycn7yfz (www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html)*.

50 "War and PC: cyberwarfare," *Jane's Defence Weekly*.

51 Siobhan Gorman, see reference #37.

52 "Cyber spies assault US power grid," *Jane's Intelligence Digest*, May 5, 2009. In July 2009, Germany said that it faced extremely sophisticated cyber-spying operations by Chinese and Russian agencies. Operational targets were industrial secrets and critical infrastructure, such as Germany's power grid; see Simon Tisdall, "Cyber-warfare 'is growing threat,'" *Guardian*, February 3, 2010, available at: *http://tinyurl.com/ylav6sg (www.guardian.co.uk/technology/2010/feb/03/cyber-warfare-growing-threat)*; and Kate Connolly, "Germany accuses China of industrial espionage," *Guardian*, July 22, 2009, available at: *http://tinyurl.com/n7ggep (www.guardian.co.uk/world/2009/jul/22/germany-china-industrial-espionage)*. It is therefore by no means unlikely that there has also been the same type of infiltration of U.S. power grids, as these other sources also seem to indicate.

53 "U.S. Steps Up Effort on Digital Defenses," *New York Times*. According to Larry Wortzel, Chinese researchers at the Institute of Systems Engineering at Dalian University of Technology have published a paper showing how to attack a small U.S. west-coast power grid; see Larry Wortzel, "China's Approach to Cyber Operations: Implications for the United States," 5.

54 Some people think that it is an exaggeration to say that China can switch off the power in different countries. I agree with that point and I am not making any such claim, but just saying that China may be able to do it in some countries. Speaking of cyber attacks on U.S. electric grids, the 2009 incident is not the first case of this kind. In April 2007, a U.S. electricity company might have been exposed to the same type of attack as those that were later alleged to have taken place. At that point in 2007, the difference was that the attackers did not come close to success with their attack; see "Total gridlock—Cyber threat to critical infrastructure," *Jane's Intelligence Review*, October 12, 2009.

55 Ibid.

56 "Cyber spies assault US power grid," *Jane's Intelligence Digest*, May 5, 2009.

57 "U.S. Steps Up Effort on Digital Defenses," *New York Times*.

58 Michael Evans and Giles Whittell, "Cyberwar declared as China hunts for the West's intelligence secrets," *Times Online*, March 8, 2010, available at: *http://tinyurl.com/y8nmzfc (technology.timesonline.co.uk/tol/news/tech_and_web/article7053254.ece)*. According to the *Times Online*, a cyberwar has now been declared: "Urgent warnings have been circulated throughout NATO and the European Union for secret intelligence material to be protected from a recent surge in cyberwar attacks originating in China," which has led to "restrictions in the normal flow of intelligence," *Ibid*.

59 U.S.-China Economic and Security Review Commission (USCC), *2009 Report to Congress of the U.S.-China Economic and Security Review Commission*, 167; "U.S.: Cyberspies Attack Joint Strike Fighter Project—Report," *Stratfor*, April 21, 2009, available at: *http://tinyurl.com/655lbou (www.stratfor.com/memberships/136342/sitrep/20090421_u_s_cyberspies_attack_joint_strike_fighter_project_report)*.

60 Dan Whitworth, "New 'Cyber Command' for US military," *BBC News*, April 22, 2009, available at: *http://news.bbc.co.uk/newsbeat/hi/technology/newsid_8012000/8012141.stm*; "U.S.: Cyberspies Attack Joint Strike Fighter Project – Report," *Stratfor*; "Computer Spies Breach Fighter-Jet Project," *Wall Street Journal*.

61 "Computer Spies Breach Fighter-Jet Project," *Wall Street Journal*.

62 Ibid.

63 "China: Pushing Ahead of the Cyberwarfare Pack," *Stratfor*.

64 Ibid.

65 Roger Boyes, "China accused of hacking into heart of Merkel administration," *Times Online*, August 27, 2007, available at: *http://www.timesonline.co.uk/tol/news/world/europe/article2332130.ece*.

http://scholarcommons.usf.edu/jss/vol4/iss2/2
DOI: http://dx.doi.org/10.5038/1944-0472.4.2.1

66 "Germany accuses China of industrial espionage," *Guardian*.

67 "US, Google and China clash over internet censorship," *Reuters*, January 13, 2010.

68 "Google China cyberattack part of spy campaign," *Washington Post*, January 14, 2010, available at: *http://tinyurl.com/635eylk (www.msnbc.msn.com/id/34855470/ns/technology_and_science-washington_post/)*; Steve Lohr, "The Lock That Says 'Pick Me,'" *New York Times*, January 18, 2010, available at: *http://tinyurl.com/ydg6x6k (www.nytimes.com/2010/01/18/technology/internet/18defend.html?ref=internet)*; Larry Wortzel, "China's Approach to Cyber Operations: Implications for the United States," 2. As stated in *Jane's Intelligence Review*, Cyberespionage is one of the main concerns Western states have regarding China, and the Google affair marks a watershed in terms of public awareness about industrial, as well as military, espionage conducted in cyberspace," cited in "Breaching protocol – the threat of cyberespionage."

69 Li Xiaokun, "Defense Ministry denies cyber attack support," *China Daily*, February 25, 2010, available at: *http://www.chinadaily.com.cn/china/2010-02/25/content_9502911.htm*. Lanxiang vocational school has denied the reports. Nonetheless, the school claims to have the world's biggest computer laboratory (confirmed by Guinness World Records) and is a huge vocational school that was established with military support, and is involved in training some computer scientists for the military; see John Markoff and David Barboza, "2 China Schools Said to Be Tied to Online Attacks," *New York Times*, February 19, 2010, available at: *http://www.nytimes.com/2010/02/19/technology/19china.html*; "Spyware programme used to attack Google linked to Beijing, report says," *Reuters*, February 23, 2010. The school's computer network is operated by a company with close ties to Baidu, the dominant search engine in China and a competitor of Google. The prestigious Shanghai Jiaotong University has a School of Information Security Engineering, as well as one of China's top computer science programs; see "2 China Schools Said to Be Tied to Online Attacks," *New York Times*; "Spyware programme used to attack Google linked to Beijing, report says," *Reuters*; see also: Bobbie Johnson and Tania Branigan, "Google attacks 'traced to Chinese schools,'" *Guardian*, February 19, 2010, available at: *http://tinyurl.com/yfatpab (www.guardian.co.uk/technology/2010/feb/19/google-attacks-chinese-schools)*.

70 "Foreign reporters' Google e-mail hacked in China," *Associated Press*, January 19, 2010.

71 "2 China Schools Said to Be Tied to Online Attacks," *New York Times*.

72 "Spyware programme used to attack Google linked to Beijing, report says," *Reuters*.

73 Ryan Paul, "Researchers identify command servers behind Google attack," *Ars Technica*, January 14, 2010, available at: *http://tinyurl.com/yhzmuo6 (arstechnica.com/security/news/2010/01/researchers-identify-command-servers-behind-google-attack.ars)*.

74 Expert in China's military James Mulvenon has previously said that China might have around 50,000 hackers enrolled; see "Breaching protocol – the threat of cyberespionage," *Jane's Intelligence Review*. It is not specified whether this is only military hackers or if private ones are also included.

75 Gerald Posner, "China's Secret Cyberterrorism," *The Daily Beast*, January 13, 2010, available at: *http://tinyurl.com/yh5ves6 (www.thedailybeast.com/blogs-and-stories/2010-01-13/chinas-secret-cyber-terrorism/)*.

76 John T. Bennett, "Chinese Buildup of Cyber, Space Tools Worries U.S.," *Defense-News*, January 13, 2010, available at: *http://www.defensenews.com/story.php?i=4452407&c=ASI&s=SEA*.

77 This box is primarily based on "Breaching protocol – the threat of cyberespionage," *Jane's Intelligence Review*. Quotations in the box are from this source.

78 "Defense Ministry denies cyber attack support," *China Daily*.

79 "Google China cyberattack part of spy campaign," *Washington Post*.

80 Bobbie Johnson, "US links China to Google cyber attacks—report," *Guardian*, February 22, 2010, available at: *http://tinyurl.com/ydgr5sr (www.guardian.co.uk/technology/2010/feb/22/internet-attacks-us-china-google)*.

81 Larry Wortzel, "China's Approach to Cyber Operations: Implications for the United States," 6. In the so-called "Google Hearing," Wortzel said that "All of this suggests that it is the Chinese military and intelligence services that are behind many of the penetrations of our defense systems," *Ibid*. He also found it very likely that the Chinese government was behind several other cyber attacks in the U.S. *Ibid*., 2–3.

82 "Google China cyberattack part of spy campaign," *Washington Post*. And in the U.S. Intelligence Community's annual threat assessment, Director of National Intelligence, Dennis C. Blair directly writes that the Chinese very actively are engaging in different forms of espionage (Dennis C. Blair, "Annual Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence," 43), and that China has "aggressive cyber capabilities" (ibid., 28).

83 "Mike McConnell on how to win the cyber-war we're losing," *Washington Post*.

84 Meanwhile, rumors have also been confirmed that foreign journalists in China have had their email accounts hacked into and private mails forwarded; see "China denies cyber spying charges, but claims highlight pursuit of unconventional strategies," *Associated Press*, September 6, 2007, available at: *http://tinyurl.com/6hmqde4 (www.theage.com.au/news/TECHNOLOGY/China-denies-cyber-spying-charges-but-claims-highlight-pursuit-of-unconventional-strategies/2007/09/06/1188783328617.html)*.

85 "Hackers warn high street chains," *BBC News*, April 25, 2008, available at: *http://news.bbc.co.uk/2/hi/7366995.stm*.

86 "China Tells U.S. to End Cold War Mentality," *AFP*, March 3, 2008, available at: *http://www.defensenews.com/story.php?i=3402950*; "'Cold War mentality' drives US cyber plan," *China Daily*, April 23, 2009, available at: *http://www.chinadaily.com.cn/world/2009-04/23/content_7707135.htm*.

87 "Electricity Grid in U.S. Penetrated By Spies," *Wall Street Journal*.

88 U.S.-China Economic and Security Review Commission (USCC), *2008 Report to Congress of the U.S.-China Economic and Security Review Commission* (Washington: U.S. Government Printing Office, 2008), 164.

89 "China's Secret Cyberterrorism," *The Daily Beast*.

http://scholarcommons.usf.edu/jss/vol4/iss2/2
DOI: http://dx.doi.org/10.5038/1944-0472.4.2.1

90 "Vast Spy System Loots Computers in 103 Countries," *New York Times*.

91 Robert S. Ross, "Here Be Dragons: Is China a Military Threat?" correspondence between Aaron L. Friedberg and Robert S. Ross, *The National Interest* 103 (Sept/Oct 2009): 30.

92 Timothy L. Thomas, "Nation-state Cyber Strategies: Examples from China and Russia," 467–469.

93 "China denies cyber spying charges, but claims highlight pursuit of unconventional strategies," *Associated Press*; "Beware the Trojan panda," *The Economist*, September 6, 2007, available at: *http://www.economist.com/node/9769319?story_id=9769319*; Office of The Secretary of Defense, *Annual Report to Congress: Military Power of the People's Republic of China 2009*, 52–53.

94 Qiao Liang and Wang Xiangsui, *Unrestricted Warfare*, Beijing: PLA Literature and Arts Publishing House, 47.

95 Australian Department of Defence, *Defending Australia in the Asia Pacific Century: Force 2030—Defence White Paper* (2009), 9.

96 Siobhan Gorman and Yochi J. Dreazen, "New Military Command to Focus on Cybersecurity," *Wall Street Journal*, April 22, 2009, available at: *http://online.wsj.com/article/SB124035738674441033.html*; "Obama Taps Cyber Security Exec as New Czar," *CBS News*, December 21, 2009, available at: *http://www.cbsnews.com/stories/2009/12/21/politics/main6008388.shtml*. In Denmark, too, according to the most recent Defence Commission, the country's military capability within CNO must be developed; see Forsvarskommissionen of 2008, *Dansk forsvar – Globalt engagement. Beretning fra Forsvarskommissionen af 2008, main volume* (Copenhagen: Danish Ministry of Defence, 2009), 101.

97 Department of Defense, *Quadrennial Defense Review Report*, 37–39.

98 Dennis C. Blair, "Annual Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence," 3; Department of Defense, *Quadrennial Defense Review Report*, 37.

99 It is important to note that just because the Pentagon does not speak publicly about this very much, it does not mean that nothing is being done; see Robert S. Ross, "Here Be Dragons: Is China a Military Threat?" 30.

Journal of Strategic Security

http://scholarcommons.usf.edu/jss/vol4/iss2/2
DOI: http://dx.doi.org/10.5038/1944-0472.4.2.1