CHINA'S CYBER INCURSIONS: A THEORETICAL LOOK AT WHAT THEY SEE AND WHY THEY DO IT BASED ON A DIFFERENT STRATEGIC METHOD OF THOUGHT

Timothy Thomas

March 2013

Synopsis: This paper discusses the strategy behind China's cyber activities. The paper examines the Chinese concept of strategy and how it motivates China's cyber actions. These actions take the form of reconnaissance and system sabotage concepts that result in the fulfillment of strategy and in the development of a preemptive and offensive information deterrence disposition.

The paper then examines China's response to the recent Mandiant security firm's report that accused the People's Liberation Army of compliance in attacking 115 US companies since 2006. China's next generation of quantum communications research is briefly discussed as well. The conclusions list the author's opinion regarding how to handle the Chinese in the future, through confrontation or dialogue, based on their thought process. This author argues for interceding into Chinese strategic concepts and changing the objective basis behind their cyber activities.

Disclaimer

The views expressed in this report are those of the author and do not necessarily represent the official policy or position of the Department of the Army, Department of Defense, or the U.S. government.

Introduction

China's invasive cyber activities make perfect sense—to them. Through extensive reconnaissance activities, China gains leverage in three areas: its ability to establish a cyber strategic advantageous posture over potential opponents; its ability to identify key nodes in an opponent's network and gain the potential ability to conduct system sabotage against them if necessary; and its ability to develop a cyber deterrence concept of Chinese-make through the construction of a new type of "show of force," such as the identification and revelation of a potential opponent's cyber geography that deters an opponent from acting. Cyber espionage activities are activated due to a specific strategic thought process and resulting paradigm that subsequently uncovers strategic opportunities.

The following article provides a potential Chinese-based thought process to explain such cyber behavior. The explanation is theoretical. It examines what cyber factors the Chinese see as exploitable, how these factors interact with strategy, why China continues to capitalize on these observations, and what the US and other nations can do to define a counterstrategy that would slow these activities. Also noted are propaganda mistakes the Chinese made when responding to the Mandiant Report, a recent report accusing a specific Chinese military unit of conducting cyber espionage against the US. These mistakes rendered the Chinese response impotent upon arrival.

What China Sees, Why They Use Cyber

An understanding of the contemporary objective factors of cyber is vital to comprehend what the PLA sees and how their concept of strategy is applied. This concept is different from the ends, ways, and means method of strategy, which is the most often cited US way of understanding the term. The 2007 People's Liberation Army (PLA) book *The Theory of Military Strategy*, as but one example, notes that "the relationship between the strategic environment and military strategy is a relationship between objective reality and subjective guidance." [1] The strategic environment refers to the "objective situation and conditions affecting national security and the situation of military struggles as a whole that present themselves in a given period of time."[2] Science and technology, the book notes, have a "propelling" effect on military strategy.

In contemporary times, a cyber strategy is the result of the creative use of subjective thought to manipulate or guide objective cyber conditions, which are the dynamic new aspects of the strategic environment. Chinese specialists do so via electron-based stratagems, and they write openly about it. For example, a packet of electrons can execute a stratagem such as "rustle the grass to startle the snake," that is, cause firewalls to alert and thus expose defense capabilities when probed.

The Chinese *Xinhua Cidian* (*Xinhua Dictionary*) defines subjective and objective factors as follows:

[1] Fan Zheng Jiang and Ma Bao An, *The Theory of Military Strategy*, National Defense University Publishing House, 2007, p. 60.
[2] Ibid.

> **Subjective refers to a person's thinking or understanding. Objective refers to the material world existing outside of a person's consciousness** [emphasis is the author's]. The relationship between subjective and objective is a dialectical unity. Objective does not rely on subjective and exists independently, it is the source of subjective, it determines subjective; subjective reflects objective, and actively reacts with objective, under certain conditions it determines the effect of objective. **The objective world is constantly developing and changing, and a person's understanding must also accordingly develop and change.**[3]

China's comprehensive view of the contemporary world, in accordance with this definition, has changed as new objective factors (in this case cyber) have emerged. In the cyber arena, objective factors include, but are not limited to, the following:

- US weaknesses in protecting its cyber systems
- anonymity associated with cyber attacks
- availability of people and equipment to be used as surrogates (hackers or servers) to mask attack vectors
- lack of rules and regulations to guide international cyber behavior
- ability to use packets of electrons as stratagems to manipulate perceptions and actions (e.g., phishing)
- long- and short-term intelligence capability of cyber reconnaissance, often without detection
- use of Chinese censorship versus US openness
- development of organizations that can create new cyber scenarios for exploitation
- focus on a code of conduct instead of the law of armed conflict by China
- development of different types of cyber geography and methods of exploiting them
- US use of dialogue instead of confrontation in regard to cyber actions
- transnational character of cyber issues
- easy access to trade secrets or intellectual property via cyber systems, to include the production of information technology items (iPhone, etc.) in China for export to the West.

Thus what China "sees" is objective cyber factors that, when the proper subjective thought is applied, help achieve equilibrium with or an advantage over competitors. More importantly, a key element of the objective factor of cyberspace is that it is invisible! Cyber is an objective factor that belongs in a whole new category. A show of force in the cyber world is very different from a show of force involving tanks. A cyber show of force can involve actually mapping and showing an opponent his **strategic cyber geography**, thereby deterring an opponent due to the exposure and exploitability of his key nodes and infrastructure. The use of tanks simply deters from a show of hardware on a local level and does not work on a strategic

[3] *Xinhua Cidian* (*Xinhua Dictionary*), 1985, p. 1106.

scale. This is why comparisons to the old concepts of land or sea boundaries are most likely inappropriate. As *The Theory of Military Strategy* notes regarding the defense of national security:

> Because of this, accurately assessing the threats and challenges confronting national security during a given period of time, scientifically predicting possible developments and change, truly taking precautions in advance and adapting beforehand, and enabling military strategy to continually become more relevant and realistic by actively adapting to the demands of the objective environment are of very important significance in effectively guiding military struggles and defending national security and development interests.[4]

Subjective thought uses and/or manipulates these objective and invisible factors to China's benefit. Subjective thought is where traditional Chinese thought (the use of thirty-six stratagems and *shi*,[5] for example) is applied. The combination of cyber's objective factors and subjective thought have enabled China to build up its digital prowess, reap a huge harvest of digital intelligence from other nations, and evade responsibility for these actions. There appears no end in sight to these activities, unless affected global powers undertake measures to disrupt these objective factors and stop the onslaught through actions not words. It is necessary to change the objective factors that China perceives.

The "why" of China's conduct of these activities is threefold. First, it does so because it can. China does not have to worry much about its cyber activities since it can claim innocence and point to the unreliability of foreign investigations, particularly in a time of anonymity or use of surrogates, a time that is, however, slowly diminishing. This absence of responsibility would be like one nation raining shells from drones on another nation, while the attacking nation continuously states "we aren't responsible" and the nation under attack has no way to prove drone ownership, thus allowing the rampage to continue.

Second, cyber reconnaissance activities allow China to obtain its end goal of establishing as decisively as possible a strategic advantage or *shi*, a term associated with a favorable disposition of forces. Cyber's anonymous character allows the Middle Kingdom's personnel to scout out key nodes and weaknesses during reconnaissance missions, to map a nation's cyber geography for exploitation, and to identify system sabotage possibilities. Uncovering weaknesses in peacetime allows for an initial advantage if war breaks out. Once a strategic advantage is established, China has the ability to "win victory before the first battle" in a future cyber conflict. That is, they have prepared the cyber battlefield ahead of time.

Third, and perhaps most important, the end result of strategy's basic objective is to make someone do something for himself that he is actually (unknowingly) doing for you. That is, the Chinese use cyber to get an opponent to make decisions seemingly for their own protection or good when in fact they are doing something for PLA or civilian cyber specialists. Chinese strategy specialist Li Bingyan offered an example of this objective with the following story:

[4] Fan and Ma, p. 59.

[5] For an explanation of the concept of *shi*, see this author's work *The Dragon's Quantum Leap*, Appendix Two. A short and concise explanation of *shi* is located on the next page.

> With regard to a strategy of making a technical opponent do something they don't want to do, Mao asked the following: 'How do you make a cat eat a hot pepper?' His answer was as follows: 'You can stuff it down his throat (the most difficult), you can put the pepper in cheese and make him swallow it, or you can grind the pepper up and spread it on his back. The latter method makes the cat lick itself and receive the satisfaction of cleaning up the hot pepper.' The cat is oblivious to the end goal. This is strategy.[6]

In other words, the object (the cat, a person) of strategy is oblivious to the end goal (to unknowingly do something for someone else). This objective can be fulfilled in the cyber age as easily as it was in the mechanized age. Phishing is a prime example of employing this thought process in the cyber age. Its goal is to make someone open an attachment he believes he is doing for his own edification or satisfaction, when in reality he is doing it for another and allowing this person access to his system.

Meanwhile, the harvesting of digital intelligence through reconnaissance continues, thereby enabling China to catch up faster with competitors and placing the nation and the PLA in a better position to, as the Chinese often note, defeat the superior when inferior. Cyber capabilities may, in fact, be a sub-department of the process known as China's Comprehensive National Power (CNP) index assessment, whereby China measures its power capabilities versus those of other nations. It is similar in concept to the Soviet, now Russian, concept known as the correlation of forces.

Establishing a Strategic Advantage

Traditional Chinese thought includes the concept of *shi*, an important strategic Chinese concept with roots as far back as the title of Chapter Five of Sun Tzu's classic, *The Art of War*. One US source defines *shi* as the strategic configuration of power or advantage.[7] Retired Chinese General Tao Hanzhang defines *shi* as "the strategically advantageous posture before a battle that enables it to have a flexible, mobile, and changeable position during a campaign."[8] The Chinese book, *Campaign Stratagems*, defines *shi* as the combination of the friendly situation, enemy situation, and the environment; as the sum of all factors impacting the performance of the operational efficiency of both sides; and as the key factor determining the rise and fall of operational efficiency.[9]

Dr. Henry Kissinger, in his book *On China*, writes that Chinese statesmanship views the entire strategic landscape as part of a single whole, where strategy is a means of "combative coexistence" with opponents. He states that "The goal is to maneuver them into weakness while

[6] Li Bingyan, "Applying Military Strategy in the Age of the New Revolution in Military Affairs," *The Chinese Revolution in Military Affairs*, ed. Shen Weiguang, New China Press, 2004, pp. 2-31.

[7] Ralph Sawyer, *The Art of War*, Fall River Press, 1994, pp. 143-147.

[8] Tao Hanzhang, *Sun Tzu's Art of War: The Modern Chinese Interpretation,* Sterling Innovation, 2007, p. 124.

[9] Zhang Xing Ye and Zhang Zhan Li, editors, *Campaign Stratagems*, National Defense University, 2002, pp. 8-18. The same character for strategic advantage or *shi* also has been translated as energy, potential, force, disposition, and momentum.

building up one's own *shi*, or strategic position."[10] A strategist's task is to analyze a situation, determine its relationship to context, and capture the direction of that evolution, Kissinger notes.[11] Certainly, China's cyber strategy fits this description. Objective factors describe the context, while subjective thought describes how these factors will be used to strategic advantage and to maneuver an opponent into weakness via cyber reconnaissance activities.

The apparent goal of the PLA's focus on cyber activities is to attain a digital quantum leap in capabilities and a strategic cyber advantage over competitors. This is accomplished when vulnerabilities are uncovered in a potential enemy's digital systems through reconnaissance activities. An advantage can also be attained by planting computer viruses that, at a specific time, could be unleashed to disable a digital system or systems. For example, a Trojan Horse is a virus that "is a form of malware that appears to perform a desirable function but in fact performs undisclosed malicious functions that allow unauthorized access to the host machine."[12] If a hacker can gain access to a server through a backdoor and insert a Trojan Horse, and execute it at a time of his or her choosing, then the virus attains the characteristics of a drawn bow, sitting there and awaiting the release of potential energy or advantage (*shi*) to achieve success.

The Chinese have written about the disposition and potential of using packets of electrons as stratagems for years. In 2002, for example, Chinese General Dai Qingmin noted that electrons can be used as carriers of strategies. They enable reconnaissance or attacks from continents away in a surreptitious manner. This can result in a quick strategic advantage. Digital-age warfare completely fits with Sun Tzu's observation that "war is such that the supreme consideration is speed." Further, Dai added that "computer network reconnaissance is the prerequisite for seizing victory in warfare. It helps to choose opportune moments, places, and measures for attack."[13]

Civilian and military hackers attempt to exploit the disposition and strategic advantage that electrons create. These activities are difficult to trace directly to the PLA or to government authorities due to the anonymous character of the Internet. This anonymity increases the *shi* (or strategic advantage) of the hacker. Further, the hacker uses packets of electrons as stratagems to change strategic advantage into a force or agent of influence to use against an opponent.

The *shi* of electrons is applicable to a state's capability to execute and conduct strategic network warfare. Objective factors to consider when employing network warfare include force capability (the strength or weakness in controlling the direction and flow of information); the amount of data possessed by combatants; the degree of network architecture redundancy (and proposed speed of recovery after being attacked); and the combat objectives and specific strategy (attack, defend, hide, move, etc.) chosen. Successfully mastering these elements can be important to the attainment of a strategic advantage.

Retired General Tao addressed the intangibles of *shi*. He wrote that a commander must make use of advantageous terrain, seize favorable opportunities for fighting, and have superiority

[10] Henry Kissinger, *On China*, Penguin Books, 2012, p. 31.
[11] Ibid., p. 30.
[12] Trojan Horse, *Wikipedia*, accessed 16 January 2009.
[13] Dai Qingmin, *Direct Information Warfare*, National Defense University Publishing House, 2002, p 96.

in the quality of troops.[14] Put in terms of the information age, this would indicate that troops must understand the terrain of the computer, seize opportunities where they exist, such as in network reconnaissance (thereby setting the stage to win the fight before the first battle), and train information technology professionals. Troops obviously have more opportunities to achieve objectives in the absence of any defining international cyber laws.

The concept of *shi* has many potential consequences beyond the military, of course. Of concern to Western societies should be the question of whether this concept can be expanded to control market societies and to manipulate the electronic flows of free societies. If so, then it seems highly possible that one well placed and educated computer specialist could serve this purpose today and stop the flow of ten thousand (or more) decisions in the market place. As General Tao notes there is a saying: "With only one man guarding the mountain pass, ten thousand men are not able to pass."[15]

System Sabotage and Cyber Deterrence

System Sabotage

The attainment of virtual *shi* or strategic advantage through extensive reconnaissance activities is the shaping mechanism that enables the use of preemptive moves and system sabotage activities at a time and choosing of the Chinese. The Chinese have noted that a post-emptive move is "not an effective way to seize the initiative on the informatized battlefield."[16] Rather, to seize the initiative and control war in the initial state of a conflict, the active offense must be emphasized, as well as system sabotage.

The book, *A Study Guide for Information Operations Theory*, described system sabotage warfare in the following manner:

> What Is System Sabotage Warfare? The basic characteristics of informatized wars are that they are guided by information and that they consist of two systems fighting each other. This is why system sabotage is so important as it is the decisive mechanism of informatized operations, and it is the basic path to victory in informatized wars.
>
> The key point to system sabotage is in 'gaining control, using precision strikes for maximum damage, and paralyzing the enemy to subjugate his will.' This primarily entails using asymmetrical operations where the emphasis is on the 'destruction' part of the equation. Methods to attack weaknesses in a system include blocking network connections, breaking down the system architecture, and lowering operational effectiveness. [17]

[14] Tao, p. 130.
[15] Tao, p. 128.
[16] Zhang Yu, Liu Sihai, and Xia Chengxiao, "On the Art of Controlling War Situation in Informatized Warfare," *China Military Science*, No. 2 2010, pp. 24-31.
[17] Xu Genchu and Dai Qingmin, *Study Guide for Information Operations Theory*, Academy of Military Science Press, November 2005, pp. 395-396.

Gaining control is achieved through the attainment of a cyber strategic advantage, while system sabotage is directly related to breaking down an opponent's system architecture. This implies attacks on key nodes.

Authors Xu Genchu and Dai Qingmin note that to make system sabotage effective there needs to be a basic mode of thinking where the Chinese "destroy before conducting war, using destruction to aid in the fight." This is because under informatized conditions the core elements and mechanisms for victory in war have undergone critical changes, with many key war systems capable of infiltration and sabotage before conflict begins in the cyber age. Obviously, conducting system sabotage means destroying the network before engaging in war.[18] For that reason, reconnaissance is so important, as it identifies the nodes to destroy and allows attackers to decide in what order.

The military press in China is often peppered with references to the system sabotage concept. Some Chinese believe that this concept is a better method of fighting in the digital age than attrition; that it utilizes both hard and soft strikes; and that it is identified as an operational pattern of war, whereas the system of systems (SoS) approach is recognized as a characteristic of war.

Both concepts, system sabotage and SoS, increase in use under informatized operational conditions. Methods are developed for employing system sabotage operations in peacetime. During field exercises, system sabotage methods are sometimes employed in the PLA's internal red versus blue exercises. The Mission Action-2010 exercises, for example, emphasized the position and role of information as the main element guiding the exercise, "firepower as the main battle in system sabotage," and the inspection and examination of system sabotage tactics, such as precision strikes and the selection of key targets, as main items to practice in peacetime.[19] It appears that the system sabotage element is becoming a key part of any planning stage in PLA operations.

Cyber Deterrence

Deterrence is another concept that is being discussed in PLA and civilian works. Non-warfare measures such as cyber have encouraged the use of military deterrence and have elevated it to a strategic level, according to some theorists.[20] The Chinese note that a cyber "show of force" (a show of force might include the ability to expose the key nodes of an opponent) enables the use of both technical and psychological pressure against an opponent. As *The Theory of Military Strategy* notes regarding information deterrence:

> At the same time, owing to the application of information technology in the field of military affairs, the degree of informatization of warfare elements is increasing day by day, the dominant role of information in warfare is growing, and the side

[18] Ibid.

[19] Chen Zhi, Pan Zhiqiang, and Gao Xiaowen," A Certain Chengdu Military Region Group Army goes to an Ancient Battlefield in the Northwest—Advancing on Helan, Honing Elite Troops," *Jiefangiun Huabao*, 18 November 2010,pp. 44-45.

[20] Fan and Ma, p. 217.

> that possesses information superiority will be able to quickly seize victory in war, thereby making information superiority itself into a deterrent force.[21]

The Chinese emphasis on the psychological quality of deterrence allows the PLA to use the cyber option so daringly in head-to-head confrontations based on risk and reward. Some theorists write that "the main consideration in deterrent war is not real-war actions…rather, the key is to cause significant awe in the adversary's psyche."[22] In *On China*, Dr. Henry Kissinger noted Mao's tendency to utilize the psychological quality of deterrence:

> For Mao, the Western concept of deterrence was too passive. He rejected a posture in which China was obliged to wait for an attack. Wherever possible, he strove for the initiative. On one level, this was similar to the Western concept of preemption—anticipating an attack by launching the first blow. But in the Western doctrine, preemption seeks victory and a military advantage. Mao's approach to preemption differed in the extraordinary attention he paid to psychological elements. His motivating force was to …change the psychological balance, not so much to defeat the enemy as to alter his calculus of risks.[23]

Technically, the more transparent the PLA can make the cyber battlefield through reconnaissance activities and the more the PLA can generate new combat power by transferring its pirating of military-industrial digits into combat equipment, the better its chance of attaining a psychological advantage and information deterrence capability. An opponent will be deterred when his risk calculus becomes problematic as a result of being confronted with an opponent with an offensive and seemingly all-knowing information image that appears realistic.

Writing in *China Military Science* in 2001, Zhao Xijun, a deputy commander of Second Artillery (responsible for nuclear weapons), defined deterrence as "military actions in the form of a show of force between countries or political groups, or an indication of their resolve and readiness to use force, intended to make an opponent not dare to take hostile action or to escalate his actions."[24] In this case, a show of force could simply be the presentation to the other side of the virtual layout of its cyber infrastructure or digital terrain. If one were to attempt to extrapolate what China's cyber deterrence theory might look like from its strategic deterrence theory, Zhao's article is an interesting contemporary start point. Zhao implies that deterrence theory is based on a combination of stratagems. These stratagems are using soft power and reconnaissance to win victory before the first battle.[25]

Zhao notes that key factors in Sun Tzu's writings that influence contemporary deterrence theory include having superior military power, being fully prepared for war, having severe measures of punishment at one's disposal, having superb skill at "attacking strategy" and

[21] Ibid.

[22] Ibid., p. 223.

[23] Kissinger, p. 133.

[24] Zhao Xijun, "Victory without War and Modern Deterrence Strategy," *China Military Science*, 2001, pp. 55-60.

[25] Ibid.

"attacking diplomacy," and making one's ideology of deterrence a lynchpin in a more complete system. All of these factors have cyber-age relevance. For example, being fully prepared for war could mean mapping another nation's cyber geography. Zhao adds that a counter deterrent capability is the most effective method to stop the aggressive attempts of powerful nations from harming China's national interests.[26]

Zhao adds that China should use an integrated deterrence approach. A single deterrent force is not sufficient to constitute effective deterrence. Comprehensive power must be employed to retain the strategic initiative. This thought brings to mind the work of Qiao Liang and Wang Xiangsui in their book, *Unrestricted Warfare*. The authors noted twenty-four different types of warfare and then theorized that a "tasty cocktail" mixture of the methods would best bring about success.[27] Thus, one might envision a cyber mixture as follows: cyber preemption plus network reconnaissance plus high-tech deception plus financial market disruption plus network deterrence, and so on in order to impose cyber deterrence. Zhao states that when striking, an offensive force must do so resolutely, threatening targets with the greatest strategic value first. When there is no smoke or gunpowder, strategy and psychology act as multipliers of power and resolve in deterrence.[28]

Editor Cai Cuihong's 2003 book, *Information Networks and International Politics*, proposed an information deterrence theory. The work views the information umbrella as more utilitarian than the nuclear umbrella. The information umbrella must be able to control information dominance (establish the strategic advantage!) and enable one side to see the adversary, while not allowing the adversary to see friendly activities. Anonymous cyber activities enable this situation, since they are roadblocks to transparency. Control over information has become a new deterrent force as a result. Cai's work notes that "the side that controls information can manipulate the start and conclusion of wars, can use informatized weapons to paralyze enemy weapons and command systems, and can destroy the enemy's precision-guided weapons."[29] Cai adds that "information network warfare under conditions of nuclear deterrence will be the new form of future international conflict."[30] The deterrent strength of China's armed forces will be balanced on the basis of its computing power, communications capacity and reliability, real-time reconnaissance capabilities, computer simulation capabilities, and other information elements. These elements can deter through misconceptions and psychological pressure.[31]

An interesting article on strategic deterrence was published in 2004 in *China Military Science*. Zhou Peng and Wen Enbin, from the Academy of Military Science, wrote that targeted deterrence can be achieved due to the controllability and flexibility of informatized measures.[32] A show of force could be presented to another country in the cyber age simply by demonstrating

[26] Ibid.

[27] Qiao Liang and Wang Xiangsui, *Unrestricted Warfare*, Pan American Publishing Company, Panama City, Panama, 2002, p. 118.

[28] Zhao Xijun.

[29] Cai Cuihong, *Information Networks and International Politics*, [publisher unknown], 2003, pp. 163-164.

[30] Ibid., p. 172.

[31] Ibid., p. 178.

[32] Ibid., pp. 20-21.

control over a network. The authors add that former Chinese President Jiang Zemin recommended elevating deterrence to the level of strategy. It should be used to contain war, delay its outbreak, or prevent its escalation. The core of new deterrence capabilities should be "assassin's mace" technologies, which would certainly fit cyber reconnaissance and digital sabotage methodologies. Due to the fast nature of high-tech wars, a war's start can have decisive significance. For that reason China "must establish an emergency mobilization combat force" if it is to unleash the deterrent effect of people's war under high-tech conditions.[33] This emergency mobilization force in the Information Age could be the cyber militias that China has developed.

A good deterrent force involves the use of nuclear deterrence, conventional deterrence, space deterrence, and information deterrence, again reminding one of cocktail warfare.[34] The authors add that "The acme of the art of strategic guidance is fully reflected in the proper selection and constant innovation of deterrence forms; it is the most real, most dynamic part of wielding strategic deterrence."[35]

The threat of system sabotage and its psychological overtone can lead to cyber deterrence. In 2007 Major General Li Deyi stated that information deterrence will rise to a strategic level close behind nuclear deterrence. New and important modes of deterrence will include information-technology deterrence, information-weaponry deterrence, and information-resource deterrence. Further, counter information deterrence will be part of China's new mode of thinking.[36] Also in 2007 Senior Colonel Deng Yifei wrote that information deterrence would be a means, behind nuclear deterrence, to achieve national strategic goals and military strategic goals. Deng believes that information has become the core concept in military thinking. Vying for information supremacy and forming information deterrence capabilities are key areas of current military thought.[37]

Also in 2007, Fan and Ma wrote on information deterrence in their work *The Theory of Military Strategy*. They divided deterrence into nuclear, conventional, information, and space forces. This division is of interest, since it clearly proposes a line of demarcation between conventional and information deterrence forces. With regard to the latter, Fan and Ma wrote the following:

> We must focus on improving information acquisition and information attack and defense capabilities, and have effective capabilities for attacking and paralyzing the enemy's basic strategic information systems. Because of this, the coordinated development of forces for information acquisition [author's note: reconnaissance?], information defense, and information offense, with strategic information warfare units making up the main part, is necessary.[38]

[33] Ibid., pp. 22-23.
[34] Zhou and Wen, p. 24-25.
[35] Ibid., p. 25.
[36] Li Deyi, "A Study of the Basic Characteristics of the Modes of Thinking in Informatized Warfare," *China Military Science*, No. 4 2007, pp. 101-105.
[37] Deng Yifei, "A Revolution in Military Thinking in the Information Age," *China Military Science*, No. 6 2007, pp. 71-78.
[38] Fan and Ma, p. 221.

In 2009 a few top nuclear generals in China wrote on information resources and the information components of weaponry as they apply to information deterrence. For example, Zhou Fangyin noted that the concept of information deterrence is defined as forcing an adversary to lay down his weapons through demonstrations or through highlighting friendly force weaponry's advanced precision under informatized conditions.[39] In 2010 Senior Colonel Yao Yunzhu, writing in the US journal, *Air & Space Power*, stated that China will continue to apply deterrence at the grand strategic level while depending more on "uncertainty" for a better deterrence effect.[40] Even though her comments were with regard to nuclear deterrence, they could easily fit an information deterrence scenario. In the age of computer hacking, "uncertainty" as to a hacker's actual identity or government connection is a common problem.

Finally, when referencing a discussion with former paramount leader of China Deng Xiaoping, Dr. Kissinger noted that Deng had proposed a preemptive policy with regard to countering any offensive moves along China's borders that could be made by the then Soviet Union. Kissinger noted that Deng's policy of preemption was an aspect of China's offensive deterrence doctrine.[41] Today, China's cyber activities, designed to develop a preemptive strategic advantage, could be viewed in the same way.

The Mandiant Report

There have been many reports of Chinese data theft, with some detailing even the methodologies involved, such as an extensive report from Northrop Grumman (2009). There were reports of Chinese attacks on *The New York Times* and *Wall Street Journal*, and there were also detailed reports of espionage and theft labeled Ghostnet, Night Dragon, and Shady Rat, among others. The report from the Mandiant security firm did not state something new when it claimed that China was conducting extensive cyber attacks against US companies. But what was new was the identification of who was conducting the attacks and the detailed forensics that identified the incursions. Finally, someone had identified the "who and how" of China's extensive piracy. This is an important step, as dialogue and agreements, at least those visible to outside viewers, have not thwarted Chinese aspirations to date in the least. Of equal importance is that China, while maintaining that the US has conducted numerous cyber attacks against it, has no "case study" on file to back up their claims. That is, there is no Google or Lockheed Martin or Northrop Grumman equivalent. The lack of such Chinese information implies that the attacks from the US could be just hackers or people from other nations using US ISPs. There is no smoking gun as with the Chinese incursions, which not only did reconnaissance work but exfiltrated files and terabytes of information.

Mandiant's Claims

Mandiant identified a group of hackers it called the "Comment Crew" that has stolen terabytes of information since 2006 from over 141 corporations. As their report noted, "the sheer scale and duration of sustained attacks against such a wide set of industries from a singularly

[39] Zhou Fangyin, "The Effect of the Information Revolution on Military Affairs and Security," Beijing *Xiandai Guoji Guanxi*, 1 August 2001, pp. 28-32.
[40] Yao Yunzhu, "China's Perspective on Nuclear Deterrence," *Air & Space Power Journal*, Spring 2011, p. 30.
[41] Kissinger, p. 364.

identified group based in China leaves little doubt about the organization beyond the group."[42] With a "well-defined attack methodology" the group stole technology blueprints, proprietary manufacturing processes, and business plans.[43] The group was identified as the People's Liberation Army (PLA) Unit 61398. Mandiant's report has a "torrent of details" that includes information on three of the hackers (code named Ugly Gorilla, Dota, and SuperHard) and photographs of one of the buildings in Shanghai where the attackers worked. Just as important, the report noted that "in a state that rigorously monitors Internet use, it is highly unlikely that the Chinese government is unaware of an attack group that operates from the Pudong New Area of Shanghai."[44]

Kevin Mandia, Mandiant's chief executive, noted that if the thefts are not coming from Unit 61398, then the "most-controlled, most-monitored Internet networks in the world are clueless about thousands of people generating attacks from this one neighborhood."[45] Mandiant's worry is that instead of stealing from companies like Coca-Cola, the focus appears to have changed to reconnoitering critical infrastructure in the US. One target, the report notes, was a company "with remote access to more than 60% of oil and gas pipelines in North America."[46] Project 2049 Institute,[47] which earlier released an excellent report on the PLA's intelligence activities, believes Unit 61398 targets the US and Canada, and is a central espionage entity. Mandiant also uncovered a China Telecom memo that discussed how it was to install high-speed fiber-optic lines for Unit 61398. Finally, Dell SecureWorks believes Comment Crew was behind the attacks known as Shady RAT in 2011 as well.[48]

China's Response to the Mandiant Report

The initial Chinese response to the Mandiant report was simply accusatory. Numerous Chinese articles stated that the allegations were groundless, irresponsible, false, and unprofessional, to name but a few. One article even asserted that "China has been too tolerant in previous Internet disputes with the US. Since China's tolerance was not appreciated by the US, China should confront the US directly."[49] There has been nothing in China's cyber activities for the US to appreciate, as the Chinese have sucked terabytes of information out of US and other nations' systems illegally. Further, the Chinese article noted that "China has no obligation to foster ties when some Americans spit on it;" and "China is not afraid of the hubbub of US public

[42] Charles Riley, "Chinese Military Engaged in 'Extensive Cyber Espionage Campaign'," at https://twitter.com/intent/user?screen-name=cnnmoneytech

[43] Ibid.

[44] Lolita C. Baldor, "US Ready To Strike Back Against China Cyberattacks," Yahoo.com, 19 February 2013.

[45] David E. Sanger, David Barboza, and Nicole Perlroth, "Chinese Army Unit Is Seen As Tied to Hacking Against US," *The New York Times*, 19 February 2013, p. 1.

[46] Ibid.

[47] The Project 2049 Institute, established in January 2008, seeks to guide decision makers toward a more secure Asia by the century's mid-point. The organization fills a gap in the public policy realm through forward-looking, region-specific research on alternative security and policy solutions. Its interdisciplinary approach draws on rigorous analysis of socioeconomic, governance, military, environmental, technological and political trends, and input from key players in the region, with an eye toward educating the public and informing policy debate. Information taken from http://project2049.net/about_us.html

[48] Sanger, Barboza, Perlroth.

[49] "Hacker Claims Reflect US Intention of Cyber Hegemony," *Global Times* Online (in English), 21 February 2013.

opinions, nor is it afraid of the US government taking actions against it."[50] This hubris was probably directed by the propaganda element of the Communist Party of China (CPC), much as it was during the Chinese response to Google when the latter accused Chinese authorities of stealing information from its sites in 2010. US analysts should take this kind of jargon for what it is—useless hyperbole designed to change the internal media's psychological atmosphere and to tell people in China that the nation is a victim, not an aggressor, of cyber incursions.

On 20 and 21 February it became clear that the Chinese had developed for internal and external consumption a set of US rationales to explain why Mandiant had accused China of hacking US systems. The clear goal was to regain control of the narrative and achieve a psychological edge over potential opponents.

The Chinese campaign countering Mandiant's report fell into one of several categories noted below. After the category are listed some of the Chinese responses supporting the category:

The Mandiant report offered a pretext for attacking China:

- The hacking accusation is used to justify a pretext for a preemptive cyber strike by the US.[51]
- The hacking accusation gives the US greater leeway to carry out its own cyber attacks.[52]

The Mandiant report is a reflection of politics:

- The accusation of a hacking threat from China was politically motivated.[53]
- The hacking accusation allows the US to attain an upper hand in Sino-US relations.[54]
- The hacking accusation allows the US government to create a potential cyber rival.[55]
- US accusations have deep social, political, national interest, and ideological motives.[56]
- The hacking accusation reveals a lack of trust in China and anxiety over national security.[57]

[50] Ibid.
[51] Zhong Sheng, "Do Not Treat Cyberspace As a War Theater: Avoid Harming Others and Damaging Oneself," *Renmin Ribao* Online, 27 February 2013, p. 5.
[52] 1st LD-Writethru-China Focus: Chinese Media Lambaste US Hacking Allegations," *Xinhua* (in English), 22 February 2013.
[53] Zhao Shengnan, China Refutes Accusations of Launching Cyberattacks on US," *China Daily* Online (in English), 20 February 2013.
[54] "2nd Ld-Writethru-China Focus: China Defense Ministry Refutes Cyber Attack Allegations," *Xinhua* (in English), 20 February 2013.
[55] Li Wei Interview, "Chinese News Live," *Feng Huang Wei Shih Tzu Hsun Tai*, 20 February, 2013.
[56] CNTV (in English), 20 February 2013.
[57] Ibid.

- The US government and private companies play good cop, bad cop with China.[58]
- The hacking accusation allows the US to use a fresh topic with which to criticize China.[59]
- The hacking accusation can be used to achieve a strategic goal of containment or deterrence.[60]

The Mandiant report offers a rationale for a US cyber force expansion:

- The hacking accusation allows the US to expand its cybersecurity forces.[61]
- The hacking accusation is a US habit that indicts other nations based on phony evidence.[62]

The Mandiant report enables a rationale for the imposition of restrictions on China:

- The hacking accusation allows the US to levy more technology restrictions on China.[63]
- The hacking accusation allows the US to limit a competitor that it sees in China's information technology and economic sectors.[64]
- The Mandiant report allows the US government to take more forceful action by applying more pressure on China.[65]
- The hacking accusation is a US attempt to attain network hegemony.[66]

The Mandiant report is a threat presentation designed to eliminate budget cuts:

- The hacking accusation allows the US to cultivate fears and mitigate military budget cutbacks.[67]
- The hacking accusation is actually a lobbying effort by groups and companies for legislation and increased funding for cybersecurity.[68]

The Mandiant report was written to protect the company's commercial software interests:

[58] CCTV-4, 20 February 2013.

[59] Ibid.

[60] Chu Lei, "Is Cyberwarfare a New Excuse for Bashing China?" *Hsiang Kang Shang Pao* Online, 21 February 2013.

[61] Zhao.

[62] Dennis Chong and Agence France-Presse, "Hkust Probes US Firm's Claims of Hacking," *South China Morning Post* Online (in English), 22 February 2013.

[6363] Ibid.

[64] CNTV…

[65] Ibid.

[66] "Hacker Claims Reflect US Intention of Cyber Hegemony," *Global Times* Online (in English), 21 February 2013.

[67] 2nd Ld-Writethru-…

[68] Zhao Shengnan, "Cyberattacks Using US IPs Target Military," *China Daily* Online (in English), 21 February 2013.

- The hacking accusation allows the US government, under pressure from businesses, to limit competition from China.[69]
- The hacking accusation allows for the US government, military, and businesses to form an alliance.[70]
- The Mandiant report is a way for the software company to promote its product.[71]
- The hacking accusation is a way to practice trade protectionism or adopt economic sanctions.[72]
- The hacking accusation uses China as a scapegoat to cover economic losses for some companies.[73]

The Incoherent Narrative: Chinese Accusations Become Counterproductive

China's arguments against the Mandiant report were the result of the production of counters (the dialectic thought process) to claims made by an opponent. These counters to the report failed to generate traction. A primary reason for this failure was the set of conflicting narratives that reduced Chinese arguments nearly to nonsense. It appeared that the arguments were developed for two audiences, China's internal population and the external world. These divisions in target audiences produced themes that contradicted one another. The following list is designed to bring these incoherent Chinese points to the reader's attention.

1. An objective fact is that China says it does not engage in cybersabotage. The Chinese state that they want to ban all cybersabotage activities,[74] yet they write about the concept widely in the military press, employing a concept known as "system sabotage," which is designed to take out cyber systems of other nations if war erupts. A description of that concept and the Chinese sources supporting it was provided above. Or consider the 2007 Chinese book *The Theory of Military Strategy*, which notes in the subsection of the chapter "The Ideology of Battle" that it is necessary to "proactively perform intensive sabotage on vital systems of the enemy."[75]

2. An objective fact, according to the Chinese, is that the US has matchless superiority and the ability to stage cyber attacks. This causes one to question that, if the PLA believes this assertion, why would Mandiant's analysis be unprofessional and unreliable? After all, US technology is superior according to the Chinese! This is apparently the use of the stratagem "appear weak when strong," since not only does China have very good hackers but also a multitude of them. These professional pirates are not affected by the same laws of armed conflict as Western nations. It is especially here that the narrative fails. It is highly unlikely that one who is superior will produce reports that are "unprofessional and unreliable."

[69] Ibid.
[70] CCTV-4.
[71] Ibid.
[72] Ibid.
[73] *Ta Kung Pao* Online, 21 February 2013.
[74] Zhao Shengnan, 20 February 2013.
[75] Fan Zheng Jiang and Ma Bao An, *On Military Strategy,* National Defense university Publishing, 2007, p. 3.

3. An objective fact is that the Chinese state they do not steal information. Yet numerous nations name only China as the perpetrator of digital theft. Terabytes of information have been stolen. Do small-time hackers need precision-targeted military information in these quantities? If the perpetrators are individuals, then why has this information not been sold on the open market by cybercriminals over the past six years? Clearly the culprit must be a nation-state that needs the information for its military-industrial complex. This information would assist the China Dream of becoming a strong military force.

4. An objective fact is that the Chinese state they want cooperation in cyber affairs yet they continually refuse to investigate foreign claims of intrusions. China's official responses from the Foreign Ministry and Defense Ministry were not those of alarm. Rather, they immediately went on the offensive after the Mandiant report was released. They chose to ignore this six-year study. There was not even a hint of a desire to investigate the charges. The Mandiant report is one of numerous accusations that have been made against the Chinese. However, in spite of foreign (some fifteen countries) evidence to the contrary, the Chinese have repeatedly failed to cooperate and investigate the accusations. Why? It must be because there is no reason to investigate if one is guilty and needs to cover one's tracks. Only the University of Science and Technology stated that it would investigate the use of its IP addresses by hackers in regard to the Mandiant report,[76] not the two ministries who were at the center of the dispute. Again, the narrative fails as the Chinese argue for cooperation yet have spurned numerous requests for investigative assistance.

5. An objective fact is that China likes to use the tactic of comparing apples to oranges to draw illogical conclusions. China was quick to describe how large the US cyber force has become in response to the Mandiant report. There is no point or relevancy to addressing size in the issue of Chinese cyber piracy. Size does not indicate criminal intent. Further, China never mentions the overwhelming size of its own force, one that has been involved in illegal operations for years and is likely much larger than the US force since it contains PLA, reserve, militia, and other cyber security forces.

6. An objective fact is that China described the Mandiant as unprofessional, lacking in facts, and lacking a technical basis to draw its conclusions; yet the report had technical detail, appeared very professionally constructed, and contained numerous facts. In a later *Wall Street Journal* report, China accused the US of attacking it. First, how could they be so sure since, earlier, Chinese analysts had stated that the Mandiant report had used unreliable ISPs to draw their conclusions? Is the "superior" US unable to use ISPs properly to expose Chinese incursions, while the less capable Chinese (according to their reports) are able to expose supposed US attacks? Second, while accusing the US, the Chinese have failed to produce a report that is even close in detail to that provided in the Mandiant report. Again, this demonstrates how poorly thought out their narrative had become and how uncooperative China has become. China wants things understood through their self-contradictory logic that holds the US responsible for attacks, while denying that the "superior" US could use the same logic to hold the Chinese responsible.

[76] Dennis Chong.

7. An objective fact is that the Chinese believe the US is unilaterally using cyberattacks to pursue trade protectionism and that this practice will incur the condemnation of the international community.[77] The US is not the only country accusing China of cyberattacks (South Korea, India, Japan, Taiwan, France, Germany, and Canada to name just a few). Only the "non-Chinese-hacked community" (Russia or North Korea?) might concur with this Chinese report, which will thus be limited in scope to China's closest partners. There has been no international condemnation to date. Again, the narrative has failed.

8. An objective fact is that China states it "will never act on the offensive side."[78] Again, Chinese open source military writings clearly state that preemption and the active offense are mandatory options in the information age, and that without these capabilities a force will lose the initiative in any cyber war. The PLA's internal writings thus describe an entirely different thought process and narrative. Further, the Chinese only appear to go on a propaganda offensive after the US accuses China of hacking. The Chinese attempted to play the sympathy card after the Mandiant report was released, noting that "we do not point fingers at the US based on the above-mentioned findings."[79] Is this because there wasn't much US activity that required finger-pointing? Another article added that one-sided media accusations jeopardize a cooperative atmosphere in cyberspace.[80] Unfortunately, Chinese piracy and their unwillingness to investigate have seriously compromised any atmosphere inviting cooperation. China states that it has established relevant laws and regulations to crack down on hacking, but, unfortunately, they are not following-up on foreign accusations of such activity. After Google accused China of hacking into its systems in 2010, China generated the same response, accusing the US of attacking Chinese systems instead of conducting an investigation.

9. An objective fact is that the PLA has been advertising for hackers for nearly a decade or working with universities to improve its cyber capabilities. The *Washington Post* noted on 20 February 2013 that a Zhejiang University recruitment post in 2004 advertised the opportunity to join China's alleged military hacker team. The notice, as translated into English by *China Digital Times*, follows:

> The Graduate School has received notice that Unit 61398 of China's People's Liberation Army (located in Pudong District, Shanghai) seeks to recruit 2003-class computer science graduate students. Students who sign the service contract will receive a 5,000 yuan per year National Defense scholarship. After graduation, students will work in the unit. Interested Zhejiang University 2003-class graduate students should please contact Teacher Peng in the Grauduate Division before May 20. (Cao Guangbiao room 108: phone: 87952168). May 13, 2004[81]

[77] Chu Lei.

[78] "1st LD-Writethru-China Focus…"

[79] "The Chinese Military Side…"

[80] Ibid.

[81] For a *Washington Post* screenshot of the post, see http://www.washingtonpost.com/blogs/worldviews/files/2013/02/unit-notic.jpg

Thus it is no wonder that foreign news media sources claim that cyber hacking teams are being established in China: several accounts of such internal advertising in China confirm this. For example, *Time* magazine described a PLA hacking contest won by Tan Dailin (aka Withered Rose), who then went on to teach hacking techniques to the PLA. A *Reuters.com* report in 2013 noted that Shanghai's Jiaotong University's School of Information Security Engineering had ties with PLA Unit 61398. Professors at Jiaotong collaborated with the PLA unit on network security and intrusion detection issues.[82] Shen Weiguang, the father of information warfare in China, developed a curriculum for an Information Security University in 2003 that included information attack and defense tactics.[83]

10. An objective fact is that there are a host of organizations in China that regulate the Internet. There is the PLA, of course, but also numerous cyber militias, reserve groups, and, of course, the Ministry of State Security. The Ministry of Industry and Information Technology is another ministry designed to control the Internet. With this number of organizations dedicated to ensuring the Internet is safe, it is highly doubtful that the Chinese could possibly not be aware of or complicit in the piracy that has occurred. If they believed in cooperation, then these organizations should have investigated international claims of piracy or espionage. Yet they did not.

11. Finally, an objective fact was the Chinese assertion that the identification of a party in an environment that is transnational, anonymous, and deceptive does not produce a reliable indictment against another nation or group or individual.[84] A professor at China's National Defense University stated that it is technically infeasible to identify the exact location of hackers,[85] while an engineer at Cina Yuntu Media Company, Ltd. said that it is impossible to locate physical addresses of attackers, and that IP addresses could be simulated or transferred.[86] A *Xinhua* report stated that hackers exploit botnets in other parts of the world as proxies for their attacks, not their own computers, as the Mandiant report implies.[87] Mandiant's findings, along with those of numerous other countries, argue otherwise. Specific people and their blogs or Internet postings were examined and described. Others were also uncovered but, due to the sensitivity of the findings, were not listed. Thus anonymity is of concern but it does not guarantee 100 percent protection. Hackers and pirates can be uncovered. And, as noted earlier, this Chinese assertion of anonymity hasn't prevented the Chinese from accusing the US of being behind cyber attacks on its systems.

12. An objective fact is that China asserts the US is behind countless cyber attacks on China. The question US analysts should pose is this: where in China are the equivalents of the wide-ranging Chinese attacks on US industry and the military (Pentagon, Lockheed Martin,

[82] Melanie Lee, "Top China College in Focus with Ties to Army's Cyber-Spying Unit," *Reuters.com*, March 23 2013.
[83] Shen Weiguang, *Deciphering information Security*, Xinhua Publishing House, 2003, p. 200.
[84] "The Chinese Military Side Continues to Refute False Accusations on 'Cyber Attacks'," *Xinhua Domestic Service*, 20 February 2013.
[85] CNTV (in English), 20 February 2013.
[86] CNTV (in English), 20 February 2013.
[87] "Hacking Allegations Against China Both Baseless and Revealing," Xinhua (in English), 20 February 2013.

RSA, Google, Northup Grumman, etc.)? There have been no accusations of this kind, indicating they don't exist. Again, the Chinese counterpropaganda comes up short.

Data piracy on the scale reported by Mandiant is a threat not only to US national security but also to our economy. In the latter case, it can result in the loss of jobs or put US companies at a competitive disadvantage. The US response to these activities has been along multiple axes that, to date, have been ineffective in stopping the Chinese data theft onslaught. A new approach should be considered, and the discussion above has offered one alternate approach to the problem.

The Mandiant security report indicated the depth of the problem in dealing with a Chinese entity that will do all it can in peacetime to achieve a strategic advantage and perhaps even impose cyber deterrence via a cyber show of force. The US will have to act decisively in the coming days if it is to achieve its goal of deterring Chinese attacks, who have no reason to stop their data piracy as long as the US response is limited to more requests for dialogue. Meanwhile, China is ratcheting up its capabilities in an area even more serious than cyber, one that many countries, to include the US, are studying—quantum computing.

Quantum Computing

Richard Meyers leads a project at the US Army Research Laboratory that involves data teleportation, perhaps the future follow-on to cyber issues. The following explanation represents the essence of why quantum communication and quantum computers, in Meyer's opinion, represent the future: they allow messages to be sent that cannot be intercepted.

> Consider a future battlefield with a Soldier, an unmanned aerial vehicle, a command and control element, and access to a satellite. 'If you put entangled atoms at each of these locations and they're moving around, then you can teleport data between the Soldier and the satellite ...you can teleport to UAVs ... you can teleport to command and control headquarters,' Meyers said. 'We think it's going to be the future for military communications. Now the strategic impact. It's possible to get information out of your location without others getting it. This is a whole new technology that will one day be common.'[88]

Currently the science of quantum teleportation "guarantees" the safe transmission of data from one site to another. Not coincidentally, this is another area where the PLA and Chinese civilians hope to gain a strategic advantage, through the development of their own homegrown quantum technology. China is currently researching this technology. Even though it is presently underdeveloped, it is still likely that it has made it on the PLA and academic watch lists as science and technology factors that will soon change the global environment.

The PLA reports that the University of National Defense Science and Technology has been conducting quantum information technology research since the 1990s. One report cited a

[88] David McNally, citing Richard Meyers in "Army Researchers Seek Secure Quantum Communications," 28 November 2012 at http://www.army.mil/article/91959/Army_researchers-seek-secure-quantum-communicat...

quantum computing laboratory that conducted a test with a laser frequency stabilizer.[89] The PLA has clearly taken an interest in quantum communications, since other PLA institutions are also studying the topic. For example, the PLA's University of Science and Technology (PLAUST) reportedly opened eleven new research areas in 2011, to include quantum communication technology.[90] China's Academy of Space Technology (CAST) has started preparatory work to establish China's first quantum remote-sensing laboratory. The aerospace community believes that remote sensing is an important area for the application of quantum information technology. Quantum information technology has been designated as one of the four key areas of scientific research in the next fifteen years.[91] Other Chinese reports on the expanded use of quantum information discussed topics such as quantum science projects and quantum mechanics experiments in space.[92]

China's civilians consider the nation as number two in the world in terms of research and development spending. China has conducted original research in quantum communications that has had an international impact.[93] State Councilor and CPC Central Committee Political Bureau member Liu Yandong noted in 2011 that quantum communications have made "fresh contributions to scientific development."[94] In 2012 she stated that quantum communication technology has important strategic significance in ensuring the safety of state information. More importantly, she made these remarks while attending a ceremony to launch the financial information quantum communication verification network.[95] With such high-level cover, it is not a surprise that China's rapid science and technology development has been tied to quantum information, as well as neutrino oscillation, nanotechnology, and stem cell studies, among others.[96]

Chinese scientists state that they have made the first experimental observation of the quantum anomalous hall (QAH) effect. The discovery, still a long way from practical application, is thought to enhance the information technology revolution through the development of low-power-consumption electronics. The QAH effect "describes how a voltage appears at both semiconductor edges when the electrons on a current-carrying semiconductor experience a force while being kept in a magnetic field."[97]

Conclusions

[89] He Shuyuan, Chen Ming, Li Zhi, and Qiao Tianfu, "Join Forces and Pool Wisdom to Forge National-Defense Equipment and Facilities…" *Jiefangjun Bao* Online, 26 July 2011, p. 8.

[90] Yang Zhijun, Yang Daichen, and Ma Shengwei, "PLA UST Promotes Integrated Development of Interdisciplinary Research," *Jiefangjun Bao* Online, 11 October 2011.

[91] *Zhongguo Hangtian Bao* Online, 25 July 2012.

[92] See, for example, "China's Space Activities in 2011," *Xinhua* (in English), 29 December 2011.

[93] Stephen Chen, "Science Chief Wants to See China Lead the Way in Scientific Breakthroughs," *South China Morning Post* Online (in English), 25 November 2012.

[94] Liu Yandong, "Striving to Break New Ground in Fundamental Research," *Qiushi* Online, 1 August 2011, No. 15.

[95] *Xinhua Domestic Service*, 21 February 2012.

[96] Cheng Yingqi, "Tianjin Meeting a Hotbed of Scientific Exchange," *China Daily* Online (in English), 18 September 2012.

[97] "Chinese Scientists Observe IT-Advancing Phenomenon," *Xinhua* (in English), 10 April 2013.

The US must confront Chinese reconnaissance efforts that attempt to establish a cyber strategic advantage that could lead to the imposition of system sabotage and cyber deterrence concepts against us. These reconnaissance efforts have been concerns of the US for the past several years. In the meantime, the Chinese have been discussing the advantages of cyber-related reconnaissance scenarios. For example, nearly thirteen years ago Chinese Colonels Qiao Liang and Wang Xiangsui wrote *Unrestricted Warfare*. What is of concern today is a scenario the authors proposed in 1999:

> If the attacking side secretly musters large amounts of capital without the enemy nations being aware of this at all and launches a sneak attack against its financial markets, then after causing a financial crisis, buries a computer virus and hacker detachment in the opponent's computer system in advance, while at the same time carrying out a network attack against the enemy…so that the civilian electricity network, traffic dispatching network, financial transaction network, telephone communications network, and mass media network are completely paralyzed, this will cause the enemy nation to fall into social panic, street riots, and a political crisis.[98]

Unfortunately the PLA, whether by design or circumstance, could be putting elements of a broad cyber strategy into place that closely resembles the colonels' scenario. The Mandiant report identified a host of industries that had been under cyber siege. These included financial services and infrastructure organizations, two key elements of the colonels' scenario. Attacks on the *New York Times* and *Wall Street Journal* in recent months could indicate attempts to reconnoiter media outlets. What US analysts should be considering is the question of "where, in such a series of steps, is China currently positioned" if this scenario or elements of it are being utilized?

To see cyber as the Chinese see cyber, one must remember the basics of the factors enumerated above. **An evaluation of cyber's objective factors is essential**. Once these factors are established, US analysts must consider how a Chinese specialist would conduct a subjective evaluation for the manipulation of these factors. It is here where thinking is as important as technology. Only then can counters be developed according to this theoretical process. Three steps in the Chinese process were highlighted as areas of concern for US cyber security:

1. China hopes to gain information through reconnaissance of an opponent's cyber system, and manipulate or influence an opponent's perceptions and technology to establish a strategic advantage. This can include the placement of viruses or Trojan Horses in enemy systems, as well as uncovering vulnerabilities, thus enabling the PLA to be in a position to "win victory before the first battle" if cyber warfare erupts.
2. China realizes that, at the appropriate time when in a state of crisis requiring a strategic advantage and preemption, reconnaissance will have enabled the conduct of system sabotage.

[98] Qiao and Wang, p. 123.

3. China thus can render a potential foe's information technology systems impotent or, after exposing all known weaknesses in such a system, use the resulting advantage to establish a cyber offensive deterrence advantage over that particular foe. That is, reconnaissance and the revelation of key nodes or devices can deter, a development not as noteworthy in the nuclear era.

Once a digital cyber strategic advantage is established, control over a potential enemy's digital systems could follow along with the ability to deter an opponent. If China is able to find vulnerabilities in another nation's cyber geography and capture or neutralize strategic information resources, then it holds the upper hand. As a developing cyber power China has attained, according to US sources, the capability to procure terabytes of information from foreign nations' information systems via reconnaissance probes. Currently there is no incentive for the Chinese to stop hacking. An examination of China's strategic thought process and paradigm could help develop appropriate counterincentives.

The US should change the objective conditions that China uses to justify to itself the right to conduct extensive reconnaissance activities. The US appears to have taken a step in the direction of a hard power response with the report that the Pentagon plans to add thirteen offensive cyber teams to its Cyber Command and another twenty-seven to support war fighting commands or to protect computer systems and data.[99] Other options advanced by US analysts include the development of alternate networks that are not accessible to the Chinese, the use of deceptive measures to expose Chinese complicity (honeypots, etc.), or the mobilization of a strong international response to China's cyber activities, since so many nations have been affected by Chinese cyber activities. These and similar items would help to undercut the objective conditions on which the PLA currently relies. China's current evaluation of these factors, since their activities have not significantly changed, does not favor Chinese piracy stopping anytime soon.

In conclusion, this theoretical view of a Chinese strategic thought process that produces cyber options offers one way of thinking about the why behind China's cyber activities as well as the how they do it. It is well-past the time to limit Chinese access to US systems. Understanding their strategic thought process could help change "what China sees" and "why they do it." US analysts need to consider such perspectives if they are to comprehend what drives the Chinese to act. Another area requiring closer scrutiny, it appears, is Chinese military literature, based on the Mandiant report's revelation of PLA Unit 61398 as a key source of many attacks. There is no secret PLA cyber formula. They write openly about system sabotage, offensive cyber operations, the use of soft force, and other such issues as well as their implementation via the use of stratagems. One simply needs to follow the Chinese way of thinking to understand why they will not stop, despite repeated warnings.

Finally, strategy, so as not to forget the ultimate utilization of the objective-subjective thought process, involves getting a cyber specialist to do something he believes he is doing for himself when actually he is doing something for a Chinese hacker (if one is to believe that the

[99] Richard Lardner, "Pentagon Forming Cyber Squads to Prevent Attacks," *The Kansas City Star*, 13 March 2013, p. A10.

PLA and others in China have applied Maoist thought to cyber). US analysts and cyber specialists should keep this Chinese concept at the fore of their analytical thoughts when investigating or when confronted with Chinese cyber incursions. The PLA has attained enough of an advantage already via reconnaissance activities without us inadvertently helping them further by not understanding their concept of strategy and its ultimate goal.