United States Marine Corps
Command and Staff College
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, Virginia 22134-5068

MASTER OF MILITARY STUDIES

TITLE: CYBER-TERRORISM AND CHINA

SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF MILITARY STUDIES

AUTHOR: LCDR LONNIE POPE

AY 07-08

Mentor and Oral Defense Committee Member: _____
Approved: ✓
Date: 29 April 2008

Oral Defense Committee Member: _____
Approved: ✓
Date: 29 April 2008

REPORT DOCUMENTATION PAGE		FORM APPROVED - - - OMB NO. 0704-0188	
PUBLIC REPORTING BURDEN FOR THIS COLLECTION OF INFORMATION IS ESTIMATED TO AVERAGE 1 HOUR PER RESPONSE, INCLUDING THE TIME FOR REVIEWING INSTRUCTIONS, SEARCHING EXISTING DATA SOURCES, GATHERING AND MAINTAINING THE DATA NEEDED, AND COMPLETING AND REVIEWING THE COLLECTION OF INFORMATION. SEND COMMENTS REGARDING THIS BURDEN ESTIMATE OR ANY OTHER ASPECT OF THIS COLLECTION OF INFORMATION, INCLUDING SUGGESTIONS FOR REDUCING THIS BURDEN, TO WASHINGTON HEADQUARTERS SERVICES, DIRECTORATE FOR INFORMATION OPERATIONS AND REPORTS, 1215 JEFFERSON DAVIS HIGHWAY, SUITE 1204, ARLINGTON, VA 22202-4302, AND TO THE OFFICE OF MANAGEMENT AND BUDGET, PAPERWORK REDUCTION PROJECT (0704-0188) WASHINGTON, DC 20503			
1. AGENCY USE ONLY *(LEAVE BLANK)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED *STUDENT RESEARCH PAPER*	
4. TITLE AND SUBTITLE Cyber-Terrorism and China		5. FUNDING NUMBERS *N/A*	
6. AUTHOR(S) LDCR Lonnie Pope			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) *USMC COMMAND AND STAFF COLLEGE* *2076 SOUTH STREET, MCCDC, QUANTICO, VA 22134-5068*		8. PERFORMING ORGANIZATION REPORT NUMBER *NONE*	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) *SAME AS #7.*		10. SPONSORING/MONITORING AGENCY REPORT NUMBER: *NONE*	
11. SUPPLEMENTARY NOTES *NONE*			
12A. DISTRIBUTION/AVAILABILITY STATEMENT *NO RESTRICTIONS*		12B. DISTRIBUTION CODE *N/A*	
ABSTRACT *(MAXIMUM 200 WORDS)* In today's society where nations continue to embrace the use of computers and technology, has resulted in weaknesses that can be exploited through cyber-terrorism. All computer systems from the personal computer, to corporate banking systems, as well as governmental and military systems are vulnerable to attack. However, the critical focus that could most effect a country like the United States are the SCADA systems that control critical infrastructures. A country or terrorist organization may not have the ability to attack the U.S. directly, but can severely cripple the U.S through these systems.			
14. SUBJECT TERMS (KEY WORDS ON WHICH TO PERFORM SEARCH) Cyber-attack, Cyber-terrorism, China, Infrastructure, SCADA systems.		15. NUMBER OF PAGES: 35 16. PRICE CODE: N/A	
17. SECURITY CLASSIFICATION OF REPORT *UNCLASSIFIED*	18. SECURITY CLASSIFICATION OF THIS PAGE: *UNCLASSIFIED*	19. SECURITY CLASSIFICATION OF ABSTRACT *UNCLASSIFIED*	20. LIMITATION OF ABSTRACT

Executive Summary

Title: Cyber-Terrorism and China

Author: LCDR Lonnie M. Pope, United States Navy

Thesis: To assess the possibility of a cyber-terrorism attack using China to explore how such an attack could affect the United States' military and U.S. civilian infrastructure.

Discussion: In today's society where nations continue to embrace the use of computers and technology, has resulted in weaknesses that can be exploited through cyber-terrorism. All computer systems from the personal computer, to corporate banking systems, as well as governmental and military systems are vulnerable to attack. However, the critical focus that could most effect a country like the United States are the SCADA systems that control critical infrastructures. A country or terrorist organization may not have the ability to attack the U.S. directly, but can severely cripple the U.S through these systems. Also, cyber-attacks are potent tools for intelligence gathering and can be a force multiplier in military operations as a strategic weapon. This paper will use China and its cyber-warfare capabilities to describe and depict the issues and concerns regarding cyber-terrorism. The next war may never see actual armies join to fight each other in battle but a war where persons on computers are able to defeat a superpower.

Conclusion: Cyber-warfare is the battleground of the future and must be taken seriously. As previously discussed, this form of warfare does not require the need to fight "man against man," yet it will certainly have a much greater affect on the United States than any other form of war previously fought. There must be a concerted effort to update current infrastructure and to train the U.S. military in methods of fighting this new form of warfare. When evaluating the threat to the United States concerning cyber-warfare: the greatest threat may not be to the U.S. military or its war fighting capabilities but to the United States' civilian infrastructure and its survival as a superpower.

DISCLAIMER

Table of Contents

ACKNOWLEGMENTS

I would like to take the time to thank the staff of the Grey Research Center for their help in this endeavor. The guidance and assistance received was extremely helpful. I would specifically like to recognize: Rachel Kingcade and Andrea Hamlen for their time and effort.

Cyber-Terrorism and China

The history of modern China began on October 10, 1911, when the Chinese people overthrew the ancient Chinese Empire, and established a republic.[1] One of the largest and most significant wars of the 20th century was the Chinese Civil War of 1930-1949. This civil war was fought between the armies of the Nationalist government of China led by President Jiang Jieshi (Chiang Kai-shek) and Communist armies under the leadership of Chinese Communist Party (CCP) headed by Chairman Mao Zedong (Mao Tse-tung). The change from an empire to a republic resulted in a radical new direction in economic, political, and social development for China. Externally, the result was a major alteration of world power bloc equations and new challenges for U.S. policymakers.[2]

Since 1949, China as a Communist Nation has done what no other Communist Nation has been able to do: It has successfully maintained its Maoist Communist ideals while establishing itself as a world power. Its culture and political system has been able to adapt and to thrive in the realm of an opposing world-view. Within the last fifty-nine years, China has come of age; however, it has had to overcome many of its scientific and technological short falls with regard to the United States by irregular means.

This thesis will focus on an ever-increasing issue of concern for the United States: Cyber-terrorism on behalf of China. According to the U.S. Federal Bureau of Investigation (FBI), cyber-terrorism is any "premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents." Unlike a nuisance virus or computer attack that results in a denial of service, a cyber-

terrorist attack is designed to cause physical violence or extreme financial harm.[3] This study will assess the possibility of a cyber-terrorism attack and will use China as an example to explore how such an attack could affect the United States' military and U.S. civilian infrastructure.

Although this study will focus on China and why it has resorted to cyber-terrorism, it is meant to be a realistic threat assessment concerning the national security of the United States. Each of the topics to be discussed has played, and will continue to play an extensive role concerning how China looks to the United States as a military and economic enemy. Only Chinese capabilities that have been reported within government agencies, academia, and the media will be presented. However, all cyber-terrorism tactics discussed will be within the capability of Chinese military.

Cyber-Terrorism:

Cyber-terrorism can be conducted on many different levels. An attack could be as simple as one person on a computer against another or a governmental agency attacking another government. Such sources or targets of attack are not limited to just the personal PC, but may include computer hardware from routers and switches to systems control and data acquisition (SCADA) systems.

This study will focus on China's use of cyber-terrorism to conduct military operations and threaten the United States' national security. When looking at cyber-terrorism there needs to be an internal focus as to what may be gained by an attack in order to know what and how to defend against that attack. Intelligence obtained by a foreign entity may be crucial in future planning, which could involve limited,

conventional, nuclear, and strategic planning against our country. Cyber-terrorism has become the easiest and most effective method of gathering intelligence in the modern era.[4] Communications, computer systems, intelligence, surveillance and reconnaissance systems vulnerabilities, because of cyber-terrorism have become a force multiplier for an enemy. The ability to gain access to these systems allows an enemy the ability to plan and execute strategic targeting of their enemies vital infrastructures.

Infrastructure:

The automation--- or *cybernation*---of the infrastructure has come about largely because it offers unmistakable economic and performance benefits. As a result, however, the United States has become a wired nation, with implications that are still not fully understood.[5]

Three current trends raise concerns about the reliability of the United States' automated infrastructure:

- Infrastructure services are becoming increasingly dependent on complex information networks that are potentially vulnerable to failure or disruption.
- The business environment is changing with deregulation, downsizing, increasing competition, and the entry of new companies into the market to provide for infrastructure services.
- Infrastructure information networks are potentially becoming more accessible even as computer intrusions, which are already quite common, are becoming increasingly sophisticated.[6]

Technological innovation, deregulation, and economic imperatives, have caused critical infrastructure systems, to become more complex and interdependent. Digital control systems-based which are based on commercial off-the-shelf hardware and software are being used to streamline network operations and reduce personnel requirements. These control networks are frequently connected by publicly accessible telecommunications systems and commercially available information technologies---the National Information Infrastructure (NII)--a trend that will accelerate as utility, transportation, and government activities eliminate antiquated, expensive private telecommunications networks. The result is a revolutionary and systemic improvement in industrial and commercial processes that has been widely recognized and exploited by both public and private sectors.[7]

However, as commercial information technologies create advantages, their increasingly indispensable nature transforms them into high-value targets. Moreover, in practice these developments have resulted in diminished systems redundancy and the consolidation of core assets, heightening the risk of catastrophic failures. The importance of cyber-security to national security was first raised in the U.S. Congress in the mid-1990s. In 1996, John Deutch, Director of the Central Intelligence Agency (CIA), testified before Congress that the number two threats to U.S. national security was cyber-attack, ranking just below weapons of mass destruction.[8] As cyber-security has come into the mainstream over the previous years, several industry groups like VeriSign which operates digital infrastructure that enables and protects billions of interactions every day across the world's voice and data networks[9] have called on the government to take action to defend the country against cyber-attack.[10]

Presidential Decision Directive 63 (PDD 63) was implemented in 1997, in an effort to protect America's critical infrastructures. This directive is the culmination of an intense, inter-agency effort to evaluate those recommendations and produce a workable and innovative framework for critical infrastructure protection. The President's policy:

- Sets a goal of a reliable, interconnected, and secure information system infrastructure--civilian and military alike.
- Immediately establishes a national center to warn of and respond to attacks.
- Addresses the cyber and physical infrastructure vulnerabilities of the Federal government by requiring each department and agency to work to reduce its exposure to new threats.
- Requires the Federal government to serve as a model to the rest of the country for how infrastructure protection is to be attained.
- Seeks the voluntary participation of private industry to meet common goals for protecting critical systems through public-private partnerships
- Protects privacy rights and seeks to utilize market forces. PDD 63 is meant to strengthen and protect the nation's economic power, not to stifle it.
- Seeks full participation and input from the Congress.[11]

Hundreds of United States information system vulnerabilities are discovered every day and many of these system vulnerabilities are directly related to U.S. national security. With regard to these vulnerabilities the United States continues to be its own worst enemy. Most of these critical vulnerabilities are posted publicly, usually on the

Internet giving hackers direct access to web pages and e-mails that contain information about United States' weaknesses. For example, Internet mailing lists routinely distribute vulnerability information and software that can be used to exploit those vulnerabilities.[12]

Once identified publicly these vulnerabilities are usually published in books, magazine, newspapers articles, electronic bulletin board messages, and a growing list of World Wide Web sites. These information sources are targeted at informing hackers, crackers, "phreakers," and, potentially, members of terrorist organizations and foreign intelligence services, about the latest methodology for staging successful cyber attacks.[13]

Many politicians like Senators Ron Wyden, Jon Kyl, and Congressman Chris Cox along with civil libertarian organization such as the American Civil Liberties Union (ACLU)[14] believe that while controls on physical borders involve the movement of mere people and things, electronic-border control would regulate information and ideas. Any attempt to block the importation or availability to information would be, by definition, an exercise of state censorship. And that, many believe, is a no-no.[15]

In a closed briefing to Congress, the CIA chief said at least a dozen countries, some hostile to the Unites States, are developing programs to attack other nations' information and computer systems. China was named at the top of the list. This also has been reflected in official thinking when the People's Liberation Daily in China stated that all a foe to the United States had to do was .... "Mess up the computer systems of its banks by high tech means. This would disrupt and destroy the United States economy."[16]

Types of Attack:

In a military sense, there are five types of cyber-attack actions: web vandalism, disinformation campaigns, gathering secret data, disruption in the field, and attacking

critical infrastructure.[17] Web vandalism includes the deactivation and defacing of official government websites. Disinformation involves the information and operation (IO) piece of a campaign, but at a much faster rate because of the Internet. The gathering of secret data is called cyber-espionage, which is much easier because it does not require a human asset to be physically within that country to obtain the secret information. Disruption of the battlefield involves targeting the enemy communications and decision-making processes that will aid in securing battlefield dominance and hindering the enemy's ability to fight effectively. Attacking a countries critical infrastructure such as the Internet/Communications systems and water systems will cause the greatest hardship to a country; thereby, limiting a country's ability to contact or operate its military affectively.

Issues:

Twenty-seven years ago, Martin Libicki, one of the earliest theorists of information warfare, stated, "If one wishes to hold off the world's superpower, and if information systems lie at the core of what makes them the superpower, then that's the place to attack."[18] This statement has only gained more relevance over time. The United States has used technology in order to achieve and maintain their superpower status.

Using the Internet has become as natural as brushing your teeth within the United States. The Internet is no longer used merely for entertainment; it now affects how Americans conduct business, purchase goods, and communicate. We use the Internet to pay our online bill payments, banking, online stock trading, and e-commerce. Currently, 48 percent of Internet users avoid making purchases online because of their cyber concerns,[19] and 73 percent of consumers say personal data theft is a deterrent to online

banking.[20] Even with such consumer skepticism, there is large economic cost saving incentives to improve cyber-security.

Richard Clarke, former Counter-Terrorism Adviser and National Security Adviser, identifies the economy as the main target of cyber-terrorism by terrorist groups, with any resulting death and destruction only considered a bonus.[21] A coordinated cyber-attack could shut down the economy by precluding electronic funds transfers and stock trading. The U.S. Cyber Consequences Unit, a division of the Department of Homeland Security (DHS), has stated that organized teams of hackers with expertise in business functions and processes could have a dramatic effect on the U.S. economy. Coordinated attacks could potentially cause billions of dollars in damage and lost profits, with sustained attacks over several days multiplying the cost manifold.[22]

Before the age of the Internet, a state could protect its interests and its economy by placing military forces between itself and its adversaries. However, there are no guided missile destroyers or M1A1 tanks in cyber-space; the old method of protecting state interests does not apply. The Internet can be used to orchestrate attacks on the U.S. economy, and military forces cannot be inserted to protect it. The civil sector is no longer a sanctuary, and a whole-hearted embrace of cyber-security is needed to prevent cyberspace from becoming the next war zone.[23]

The most common type of computer that automates daily tasks is called a supervisory control and data acquisition (SCADA) system. SCADA systems monitor and control the operation of critical infrastructure including traffic lights, water pumps, oil pipelines, dams, and the electrical grids. These SCADA systems are vulnerable to Cyber-attack--particularly if connected by a network--and the critical infrastructure within the

United States is not prepared to detect or respond to a widespread cyber-attack. The problem becomes exponentially worse if SCADA systems are connected via the public Internet rather than private networks because thus allowing direct public access without the security of a private and isolated network.[24]

Vulnerability:

> Critical infrastructure is defined in the USA PATRIOT Act as:
> Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.[25]

As a result of the current focus on terrorist threats to the United States, Congress has held several hearings regarding the vulnerability of critical infrastructure. In most cases, industry representatives claim to be prepared for any attack, while government and academic studies question preparedness. At the President's direction, an interagency group reviewed the cyber threat to the U.S. and identified options regarding how best to integrate U.S. Government defensive cyber capabilities; how best to optimize, coordinate and de-conflict cyber activities; and how to better employ cyber resources to maximize performance. This review led to the January 2008 issuance of NSPD-54/HSPD-23, which direct a comprehensive national cyber-security initiative. These actions will help to deter hostile action in cyber space by making it harder to penetrate U.S. networks.[26] For the reason that all critical infrastructures rely upon computers, and much of the controlling computers systems rely upon SCADA systems for automation.[27]

SCADA systems have been designed for operational speed and functionality, with security being an afterthought, if even considered at all.[28] The systems have also been designed for interoperability so that new equipment can be easily integrated into existing

networks. This has resulted in SCADA systems around the world similar in design and operation. Since these systems are not unique to U.S. critical infrastructure, their design is available throughout the world. Moreover, plans for attack on U.S. infrastructure can be tested on similar, readily available, foreign SCADA systems with reasonable assurance of success when used against the United States.[29]

Cyber-attack: Military Operations

The military and the organizations that support the Department of Defense are considered high-value targets. Targeting these components can disrupt military operations and is considered to be a high priority for obtaining information concerning war plan scenarios, operational doctrine, and weapons research and development. Department of Defense (DoD) computer systems have been continuous targets for cyber-attack, causing the government to implement rigorous information assurance programs. Although much progress has been made to strengthen cyber-security, cyber-attacks still occur regularly. In 2005, the Pentagon alone logged more than 79,000 attempted intrusions.[30] Because of the rate at which technology progresses and cyber-attacks become more sophisticated, DoD may always be struggling to provide a level of cyber-security adequate to counter the threat.[31]

DoD estimates that it operates between two and three million computers, 100,000 local area networks, and 100 long-distance networks, including vital war fighting networks such as the Global Command and Control System and the Joint Worldwide Intelligence Communication System.[32] The sheer size of DoD's networks makes them significant targets--even if the nature of the data and communications they transmit are disregarded. Securing such a large number of computers and networks is no easy task--

the opportunities for cyber-attack grow exponentially as the network grows--but securing these networks is vital to national security. The task of securing these networks becomes more complicated as DoD networks integrate with civilian infrastructure. Most unclassified DoD networks are highly dependent upon civilian infrastructure,[33](the Internet) and approximately 95 percent of unclassified communications travel outside of DoD networks.[34]

As cyber-attacks grow in sophistication and are employed as a weapon of warfare, these attacks will have a significant impact on military planning. Martin Libicki warns that DoD "must assume that any enemy it engages will attack [its] computers to disrupt military operations."[35] The government has also warned of cyber-attack against the U.S. homeland in response to conventional military action abroad.[36] The threat of cyber-attack as retaliation for military action demands cyber-security defenses to protect the homeland and its population, as well as offensive capabilities to help deter attacks.

Cyber-attack may also blur the line between what may have been a civilian or military target. The source of cyber-attack can be difficult to discern. Attacks may be targeted at civilian infrastructure but carry serious implications for national security, such as coordinated attacks on the U.S. banking system. Because of the lack of current legal precedence concerning the Internet, the traditional distinctions of civilian versus military and domestic versus international jurisdiction become severely muddled.[37] A swift and just response to cyber-attack incidents requires that issues of jurisdiction must be resolved quickly and accurately to ensure proper apprehension and prosecution of the attackers.[38]

The term net-centric warfare refers to the evolution of a system of intelligence sensors, command and control systems, and precision weapons that enabled enhanced situational awareness, rapid target assessment, and distributed weapon assignment. In essence, [net-centric warfare] translates information superiority into combat power by effectively linking knowledge entities in the battle-space[39] --by enhancing the capability to connect military assets via computer and communication networks; thereby, allowing the system to operate similarly to the Internet. Full Spectrum Dominance describes the ability of the U.S. military to dominate the battle-space from peace operations through to the outright application of military power that stemmed from the advantages of information superiority.[40]

China:

China as a nation has continued to grow economically and militarily, but not at the same rate as the United States. This lagging military capability has led China to look at other methods of bolstering or reinforcing its war-fighting capabilities. China sees the United States as its principle antagonist in the twenty-first century. Chinese military leaders and policy makers have made an effort to apply lessons learned from the Persian Gulf War's show of American military might. The heated Chinese debate about how to gain a military advantage over the United States produced a partial answer in *Unrestricted Warfare*, written by two People's Liberation Army (PLA) Colonels, Qiao Liang and Wang Xiangsui.[41] China has looked to asymmetrical warfare to help alleviate its military shortfalls by electing to formulate and explore methods of countering an adversary's strengths by focusing on their weaknesses.

China continues to make viable attempts to gain access to America's sensitive information. The motives of these so-called "red hackers," described as a nebula tolerated or manipulated by the Chinese Communist Party, remain unclear. Is it espionage, a desire to do harm, or do these red hackers simply want to demonstrate a particular capability or vulnerability? No matter the intention, the United States has given this offensive, which has targeted the U.S. Defense Department since 2001, the code name "Titan Rain."[42]

In the book *Unrestricted Warfare,* the authors note having watched Moscow spend itself into oblivion trying to win the Cold War arms race, and that they will seek to avoid the same mistake.[43] Instead, a digital attack would give China a significant asymmetric advantage and could even bring about the defeat of the United States. China has therefore been making large investments in new technology for the Peoples Liberation Army (PLA) and has established a special information-warfare group to coordinate national offense and defense. China experts in the Pentagon refer to these efforts as the creation of "The Great Firewall of China." Part of the reason for such aggressive action is China's belief that it is already under cyber-attack by the Unites States.[44]

For almost two decades the PLA, China's military, has been undergoing a massive transformation. Throughout the Cold War, the PLA consisted primarily of lightly armed infantry soldiers, a force that--although massive in number--was not of sufficient quality to take on the world's superpowers. Although the bulk of the PLA remains lightly armed infantry, the Chinese military has made dramatic advances in its technology since the end of the Cold War. At the forefront of China's military

transformation are high-tech capabilities including ballistic missiles, a blue-water navy, and information operations.

China's focus on Information Operations (IO) requires the PLA to adopt two measures that will allow it stand up against the great militaries of the world. First, mature IO capabilities will help in creating and maintaining a modern C4ISR infrastructure, something the PLA is sorely missing. Modern C4ISR allows the coordination of large numbers of forces across large geographic areas, and as well as synthesizes information to hasten the pace at which a force can advance. Without such capabilities, power projection is not possible and the PLA is restrained to operating close to home. Second, mature IO capabilities are an offensive weapon for use against other technologically advanced and information dependent militaries.[45] For China, an advanced Cyber-attack capability will provide an enhanced capability against an enemy at home or abroad.

Chinese IO:

Information operations are a popular topic within Chinese military publications, but the PLA has yet to develop a uniquely Chinese concept of IO. For the most part, the Chinese concept of IO closely follows the U.S. model with two exceptions. First, the Chinese place far greater emphasis on integrating Electronic Warfare (EW) with computer network attack (CNA).[46] The United States does not currently use CNA as an offensive weapon on the battlefield and relies much more on the EW portion with regards to battle. The reason for this may be due to the civil statutes, which prohibit such practices within the United States. A larger emphasis on CNA within the Chinese military publications may seem trivial at first, but clearly indicates intent to employ

cyber-attack against the United States at home and on the battlefield. Given the vulnerabilities of the U.S. critical infrastructure and military to cyber-attack, the Chinese emphasis on CNA becomes cause for alarm.

The second notable modification to the Chinese concept of IO is the influence of strategy.[47] U.S. warfighting tactics are highly focused on and driven by technology. Military planners in the United States may study classic works of military strategy, but by the nature of U.S. society and the military causes them to think in terms of technology--every military problem has a technological answer. The PLA, in contrast, is focused on and driven by strategy. Chinese military planners think in terms of stratagems, and are heavily influenced by ancient Chinese military art. Sun Tzu has been a favorite of U.S. military IO theorists for years, but the Chinese live by his advice as part of their ethos within there daily lives. Chinese IO theorists are also heavily influenced by the 36 stratagems, a collection of Chinese strategic thoughts dating back to Sun Tzu's era. Military deception is a popular theme within the 36 stratagems, and Chinese theorists view cyber-attack as a playground for such concepts. In the Chinese view, utilizing such classic stratagems within cyber-space will give them the upper hand against an unsuspecting opponent.[48]

Mao Zedong's concept of Peoples War is receiving a new life because of China's IO ambitions. Chinese IO theorists have suggested forming civilian CNA squadrons to compliment PLA forces. Having a vast quantity of civilian "reserves" would allow the Chinese to increase the level of cyber-attacks as needed, as well as guarantee the raw computing power needed to launch widespread attacks. Waging warfare with an army of citizens with laptops is beyond the comprehension of Western thinkers, but the Chinese

are banking on the winner of a cyber-war being the side that is able to bring the most computing power to bear upon the other.[49]

While U.S. theorists focus almost exclusively on targeting the military of an adversary, the Chinese have their eyes on economic, political, and societal targets. The Chinese realize that they cannot threaten other countries like other superpowers because of their currently limited nuclear force. Although still a threat, the small number of nuclear weapons in the Chinese arsenal are not capable of credibly threatening destruction of the United States. However, Chinese cyber-attack capabilities are capable of credibly threatening the United States on a large enough scale. By targeting U.S. critical infrastructure and threatening the economy and the ability of the government to provide for its citizens, the Chinese believe they have found a strategic weapon with the equalizing power that nuclear weapons gave the United States and Russia during the Cold War.[50]

The PLA:

The PLA, in a short period of time (ten years) has been able to transform 15 percent of its forces into modern units supported by high-tech weaponry.[51] This transformed "army within and an army" is designed for joint attacks conducted at lightening speed similar to the U.S military operations in Iraq in 1991 and 2003. The PLA had three original branches: the Army(PLA), Navy(PLAN), and the Airforce(PLAAF). The next step in Chinas' military transformation was the creation of a fourth branch within the PLA dedicated to cyber-warfare.[52] The PLA has already created cyber-warfare units within its ranks and reserve forces, but creating a distinct branch for cyber-warfare will enable autonomous "cyber actions" on a large scale. The creation of a

cyber-warfare branch within the PLA is another testament to the stock Chinese theorists put into cyber-attack.

The Chinese view cyber-attack as a force multiplier and have been working it into military plans and exercises for the past few years.[53] An exercise conducted in December 1999 included cyber-warfare units conducting network attack and defense, radar reconnaissance, and electronic countermeasures, in support of an enforced blockade of an island.[54] China may well use their cyber-attack capabilities to deter the United States in the same manner that the United States used nuclear weapons to deter the Soviet Union during the Cold War.

Chinese Cyber-Attacks:

The Chinese are known to regularly target U.S. defense contractors and national laboratories such as the Los Alamos National Laboratory and Lockheed Martin. Numerous attacks over the past decade against computers in the United States and Japan have been traced to China.[55] The latest report of an intrusion was a Federal Government Nuclear Weapons Laboratory at Oak Ridge National Laboratory in Tennessee on 10 Dec 2007: linked directly to Chinese IP addresses.[56] These attacks have been mainly reconnaissance and espionage in nature, and were designed to aid Chinese military transformation by gaining technical data on the U.S. nuclear arsenal and weapon systems.

The United States and China have also fought "cyber battles" in the past. The *Chinese Liberation Army Daily* reported that such a battle occurred on 27 July 1999 following the 8 May bombing of the Chinese embassy in Yugoslavia. The Chinese initiated the "battle" by altering the webpage of the U.S. embassy in Beijing, followed by more volleys, which resulted in the denial of service on several U.S. political and military

websites. Nearly 300 civilian website servers were affected; thereby, over-burdening U.S. unclassified military email servers with large volumes of spam and viruses attached to emails. However, the *Chinese Liberation Army Daily* did not report U.S. retaliatory actions during the skirmish.[57]

China's Warfare Philosophy:

"Fighting the Fight that Fits One's Weapons" and "Making the Weapons to Fit the Fight"

The Chinese warfighting strategies, "fight the fight that fits one's weapons" and "build the weapons to fit the fight" demonstrate the distinction between traditional warfare and future warfare, while highlighting the relationship between weapons and tactics in the two kinds of war. The former reflects the involuntary or passive adaptation of the relationship of man to weapons and tactics in war that takes place under natural conditions. While the latter suggests the conscious or active choice that people make regarding the same proposition when they have entered a free state.[58]

In the history of warfare, the first person credited with using principles to regularize methods of fighting should be Sun Tzu. He advocated principles such as, "know the enemy and yourself and in a hundred battles you will never be defeated," "strike where the enemy is not prepared, take him by surprise," and "avoid the solid and strike the weak." Modern strategists still follow these principles.[59]

From China's perspective, everything that can benefit mankind can also harm him. This is to say that there is nothing in the world today that cannot become a weapon, and this requires that our understanding of weapons must have an awareness that breaks

through all boundaries. As China sees it, a single man-made stock-market crash, a single computer virus invasion, or a single rumor or scandal that results in a fluctuation in the enemy country's exchange rates or exposes the leaders of an enemy country on the Internet, all can be included in the ranks of new-concept weapons. What must be made clear is that the new concept of weapons is in the process of creating weapons that are closely linked to the lives of the common people.[60]

China believes that the appearance of new-concept weapons will definitely elevate future warfare to a level that is difficult for the common people--or even military men--to imagine. Then the second thing China would say: New concept weapons will cause ordinary people and military men alike to be greatly astonished at the fact that commonplace things that are close to them can also become weapons with which to engage in war. The Chinese believe that in the future that quite a few gentle and kind things will take on offensive and lethal characteristics.[61]

Conclusion:

Cyber-terrorism, cyber-attack, or cyber-warfare, no matter what the flavor or punch line of the day, is a threat to the United States. The United States' development and reliance on technology has aided in its development as a superpower. However, overreliance on this technology may also lead to its demise.

This study is meant to be a realistic look at the weakness of the U.S. infrastructure systems with regards to China. Yet, this study could readily be applied to any technically sophisticated individuals or nations. There are still many issues regarding state security that the United States must face. There are many lurking threats, which must also be accounted for. There continues to be issues with rogue states like North Korea or

terrorists who have access or are attempting to gain access to weapons of mass destruction (WMD). Although these issues are certainly a threat to security, the U.S. cannot allow these threats to overshadow the threat that China now poses with its cyber-warfare knowledge and capability.

The nature of warfare may never change, but the character of warfare is ever changing. In history, when there has been change in the character of warfare there has been very dramatic and damaging results. The United States is experiencing these issues currently by the change of character within Iraq. If plans or preparations are not made ahead of time concerning cyber-warfare then the United States will be fighting a new character of war from which it may never recover. Cyber-warfare is the battleground of the future and must be taken seriously. As previously discussed, this form of warfare does not require the need to fight "man against man," yet it will certainly have a much greater affect on the United States than any other form of war previously fought.

There must be a concerted effort to update current infrastructure and to train the U.S. military in methods of fighting this new form of warfare. When evaluating the threat to the United States concerning cyber-warfare: the greatest threat may not be to the U.S. military or its war fighting capabilities but to the United States' civilian infrastructure and its survival as a superpower.

Notes

[1] Trevor Dupuy, The Chinese Civil War (New York: Franklin Watts Inc, 1969), 4.

[2] Gary Bjorge, Moving the Enemy: Operational Art in the Chinese PLA's HUAI HA Campaign (Fort Leavenworth Kansas: Combat Studies Institute Press, 2003), 1.

[3] Electronic, What is cyberterrorism? - a definition from Whatis.com (http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci771061,00.html)., 2/25/2008

[4] Electronic, Internet security Alliance- ISA Chairman Ken Silva before House Government Reform Committee, (http://www.isalliance.org/content/view/147/295/)., 2/25/2008

[5] Yonah Alexander and Michael Swetnam, Cyber Terrorism and Information Warfare (Dobbs Ferry, New York: Oceana Publications, Inc, 1999), 461.

[6] *Ibid,* p. 462.

[7] Louis J. Freeh, "Threats to National Security," In Cyber Terrorism and Information Warfare , edited by Yonah Alexander and Michael Swetnam, (Dobbs Ferry, New York: Oceana Publications, Inc, 1999), 539.

[8] Martin Libicki, *Defending Cyberspace and other Metaphors* (Washington D.C.: National Defense University Press, 1997), 9.

[9] Electronic, Internet security Alliance- ISA Chairman Ken Silva before House Government Reform Committee, (http://www.isalliance.org/content/view/147/295/)., 2/25/2008

[10] Grant Gross, "Call for Homeland Security Cybersecurity Improvements," *PC World Magazine,* 19 July 2005

[11] Yonah Alexander and Michael Swetnam, 180.

[12] Louis J. Freeh, "Threats to National Security," In Cyber Terrorism and Information Warfare , edited by Yonah Alexander and Michael Swetnam, (Dobbs Ferry, New York: Oceana Publications, Inc, 1999), 540.

[13] *Ibid*

[14] Electronic, A bill to Defeat Internet Jamming and Censorship (S.3093), (http://www.fas.org/sgp/congress/2002/s3093.html)., 2/25/2008.

[15] Simson Garfinkel, "Leaky Cyber Borders," *Technology Review*, June 2002, Vol. 105, Issue 5, p. 2.

[16] Louis J. Freeh, 540

[17] The Center for the Study of Technology and Society, *National Security special Focus: Cyberwarfare* (Washington D.C.: The Center for the Study of Technology and Society, 2001)

[18] Martin Libicki, *The future of Information Security* (Washington D.C.: National Defense University Press, 1981).

[19] Grant Gross, "Improve Cybersecurity, Group Urges Feds: Vendor Alliance Gives low Marks on Progress, Points to Survey of Customer Concerns," *PC World online*, 29 November 2005.

[20] Anush Yegyazarian, "Security by Numbers," *PC World Online*, 3 October 2005.

[21] John Rollins and Clay Wilson, Terrorist Capabilities for Cyberattack: Overview and Policy Issues. (Washington D.C.: Congressional Research Service, Division of Foreign Affairs, Defense and Trade, 20 October 2005. P. 3, RL33123.

[22] Grant Gross, "Security Expert: More Sophisticated Net Attacks Likely," *PC World Online*, 29 November 2005.

[23] Richard Hayes and Gary Wheatley, "Information Warfare and Deterrence." *Strategic Forum* 87, October 1996.

[24] Grant Gross, "Call for Homeland security Cybersecurity Improvements: Recovery Plan Needed for Widespread Attack on the Internet, Senate Committee Told," *PC World Online*, 19 July 2005.

[25] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT0 Act, P.L. 107-56, Title X, Section 1016.

[26] Electronic, Terrorism, (http://merlin.ndu.edu/index.cfm?secID=149&pageID=3&type=section#added)., 2/26/2008

[27] Dana Shea, Critical Infrastructure: Control Systems and the Terrorist Threat (Washington D.C.: Congressional Research Service, Division of Resources, Science, and Industry, 20 January 2004), P. 1, RL31534.

[28] *Ibid,* p. 4.

[29] *Ibid*, p. 5.

[30] Electronic, China's Cyber Army Is Preparing To March on America, says Pentagon « Status of Chinese People, (http://chinareview.wordpress.com/2007/09/08/chinaas-cyber-army-is-preparing-to-march-on-america-says-pentagon/),. 2/26/28.

[31] Robert Dacey, Information Security: Progress and Challenges to an Efeective Defense-wide Information Assurance Program (Washington D.C.: General Accounting Office, March 2001), P. 3 and 7, GAO-01-307.

[32] Robert Dacey, 5.

[33] Rollins and Wilson, 19.

[34] Libicki, Defending Cyberspace, 13.

[35] *Ibid*, p. 9.

[36] Grant Gross, "Air force will Guard Cyberspace: New Mission Space Stakes First Claim by Military Service, *PC World Online*, 9 December 2005.

[37] Electronic, The dogs of Web War-January 2008, (http://www.afa.org/magazine/jan2008/0108dogs.asp)., 2/26/2008.

[38] Robert McMillan, "Cyberthreats: Fluid and Far Reaching," *PC World Online*, 15 February 2006.

[39] David Alberts, john Garstka, and Frederick Stein, Network Centric Warfare: Developing and Leveraging Information Superiority (Washington D.C.: Department of Defense Command and Control Research program, 2003), P. 2.

[40] Electronic, Network-centric warfare (NCW), (http://en.wikipedia.org/wiki/network-centricwarfare?oldid=187678326)., 2/26/08.

[41] James Adams, "The Weakness of A Superpower," *Foreign Affairs*, May/Jun 2001, Vol. 80, issue 3, p. 4.

[42] Issabelle Mandruaud, "France Targeted by Chinese Hackers," *World News Connection*, 10 September 2007.

[43] Qiao Liang and Wang Xiangsui, *Unrestricted Warfare*, (Beijing: PLA Literature and Arts Publishing House, February 1999), p. 166.

[44] James Adams, 5.

[45] Libicki,

[46] Timothy Thomas, "Chinese and American Network Warfare," *Joint Forces Quarterly* 38 (Summer 2005), p. 77.

[47] *Ibid,* p. 82.

[48] Timothy Thomas, Like Adding Wings to the Tiger: Chinese Information Theory and Practice (Fort Leavenworth, KS: Foreign Military Studies, 2003).

[49] *Ibid*

[50] *Ibid,* p. 83.

[51] Robert Marquand, "Chinese Build high-tech Army Within an Army," *Christian Science Monitor online*, 17 November 2005.

[52] The Center for the Study of Technology and Society, *National Security Special Focus: Cyberwarfare*, 2001.

[53] *Ibid*

[54] *Ibid*

[55] *Ibid*

[56] Electronic, Cyber Attack on Nuclear Lab May Be From China - Security - IT Channel News by CRN and VARBusiness, (http:///www.crn.com/security/204800514)., 2/26/2008

[57] Thomas

[58] Qiao Liang and Wang Xiangsui, p. 19.

[59] *Ibid,* p. 204

[60] *Ibid,* p. 25.

[61] *Ibid,* p. 26.

Bibliography

"AFP: French Government Falls Prey to Cyber-Attacks 'Involving China'." World News Connection (09/08, 2007) (accessed 11/1/2007).

"AFP: PRC FM Spokesman: China also 'Victim' of Cyber Attacks." World News Connection (09/11, 2007) (accessed 11/1/2007).

"AFP: PRC Military Successfully Hacks into Pentagon Computer Network." World News Connection (09/04, 2007) (accessed 11/1/2007).

"China Post: Hacked." World News Connection (10/13, 2007) (accessed 11/1/2007).
"CNA: China shows True Colors by Hijacking U.S. Search Engines: Gio." World News Connection (10/19, 2007) (accessed 11/8/2007).

"CNA: China shows True Colors by Hijacking U.S. Search Engines: Gio." World News Connection (10/19, 2007) (accessed 11/1/2007).

Electronic, What is cyberterrorism? - a definition from Whatis.com (http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci771061,00.html,. 2/25/2008.

Electronic, Internet security Alliance- ISA Chairman Ken Silva before House Government Reform Committee, (http://www.isalliance.org/content/view/147/295/)., 2/25/2008.

Electronic, Internet security Alliance- ISA Chairman Ken Silva before House Government Reform Committee, (http://www.isalliance.org/content/view/147/295/)., 2/25/2008.

Electronic, A bill to Defeat Internet Jamming and Censorship (S.3093), (http://www.fas.org/sgp/congress/2002/s3093.html)., 2/25/2008.

Electronic, Terrorism, (http://merlin.ndu.edu/index.cfm?secID=149&pageID=3&type=section#added)., 2/26/2008.

Electronic, China's Cyber Army Is Preparing To March on America, says Pentagon « Status of Chinese People, (http://chinareview.wordpress.com/2007/09/08/chinaas-cyber-army-is-preparing-to-march-on-america-says-pentagon/),. 2/26/28.

Electronic, The dogs of Web War-January 2008, (http://www.afa.org/magazine/jan2008/0108dogs.asp)., 2/26/2008.

Electronic, Network-centric warfare (NCW), (http://en.wikipedia.org/wiki/network-centricwarfare?oldid=187678326)., 2/26/08.

Electronic, Cyber Attack on Nuclear Lab May Be From China - Security - IT Channel News by CRN and VARBusiness, (http:///www.crn.com/security/204800514)., 2/26/2008.

"French Defense Official Confirms 'Serious' Cyber-Attacks by Chinese Hackers." World News Connection (09/10, 2007) (accessed 11/1/2007).

"The Mouse that Roared." Global Agenda (09/15, 2007): 2-2 (accessed 11/1/2007).

"Pentagon did Not Confront China Over Hacking Attack." East-Asia-Intel Reports (09/12, 2007): 1-1 (accessed 11/1/2007).

"PRC FM Spokesman: Claims of PRC Network Attacks of Foreign Web Sites 'Groundless'." World News Connection (09/06, 2007) (accessed 11/1/2007).

"Report Downplays Danger of Chinese Hacker Attacks on Computer Systems." World News Connection (09/20, 2007) (accessed 11/1/2007).

"ROK Daily: China Wants Dominance in Cyber Space." World News Connection (09/21, 2007) (accessed 11/1/2007).

"Some Experts Question Activitities of China's 'Patriotic' Hackers." World News Connection (10/07, 2007) (accessed 11/1/2007).

The Center for the Study of Technology and Society, *National Security special Focus: Cyberwarfare* (Washington D.C.: The Center for the Study of Technology and Society, 2001).

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT0 Act, P.L. 107-56, Title X, Section 1016.

"Xinhua: China's Anti-Cyber Virus Authorities Warn of New Virus Transmitted." World News Connection (10/14, 2007) (accessed 11/1/2007).

"Xinhua: German Businessmen Warn Against Fears of China." World News Connection (09/01, 2007) (accessed 11/1/2007).

"AFP: PRC FM Spokesman Says Hacking Illegal After Alleged Attacks on US Computers." World News Connection (12/13, 2005) (accessed 11/1/2007).

Adams, James. "Virtual Defense." Foreign Affairs 80, no. 3; 3 (2001): 98-112 (accessed 11/1/2007).

Adams, James. "The Weakness of A Superpower," *Foreign Affairs*, May/Jun 2001, Vol. 80, issue 3, p. 4.

Alberts, David, John Garstka, and Frederick Stein, Network Centric Warfare: Developing and Leveraging Information Superiority (Washington D.C.: Department of Defense Command and Control Research program, 2003), P. 2.

Alexander, Yonah and Michael Swetnam, Cyber Terrorism and Information Warfare (Dobbs Ferry, New York: Oceana Publications, Inc, 1999), 461.

Blitzer, Wolf, Carol Costello, Abbi Tatton, Tom Foreman, MilesO'Brien, Jack Cafferty, Brian Todd, et al. "Steve Fossett Missing; Hacker Attack on Pentagon."

Anush Yegyazarian, "Security by Numbers," *PC World Online*, 3 October 2005.

Dacey Robert. Information Security: Progress and Challenges to an Efeective Defense-wide Information Assurance Program (Washington D.C.: General Accounting Office, March 2001), P. 3 and 7, GAO-01-307.

Freeh, Louis J. "Threats to National Security," In Cyber Terrorism and Information Warfare , edited by Yonah Alexander and Michael Swetnam, (Dobbs Ferry, New York: Oceana Publications, Inc, 1999), 539.

Freeh, Louis J. "Threats to National Security," In Cyber Terrorism and Information Warfare , edited by Yonah Alexander and Michael Swetnam, (Dobbs Ferry, New York: Oceana Publications, Inc, 1999), 540.

Bjorge, Gary. Moving the Enemy: Operational Art in the Chinese PLA's HUAI HA Campaign (Fort Leavenworth Kansas: Combat Studies Institute Press, 2003), 1.

Garfinkel, Simson ."Leaky Cyber Borders," *Technology Review*, June 2002, Vol. 105, Issue 5, p. 2.

Garfinkel, Simson. "Leaky Cyber Borders." Technology Review 105, no. 5; 5 (06, 2002): 31 (accessed 11/1/2007).

Greenemeier, Larry. "Cyberwarfare: By Whatever Name, it's on the Increase." InformationWeek no. 1145 (Jul 2-Jul 9, 2007): 32,

Gross, Grant . "Call for Homeland Security Cybersecurity Improvements," *PC World Magazine*, 19 July 2005

Gross, Grant. "Improve Cybersecurity, Group Urges Feds: Vendor Alliance Gives low Marks on Progress, Points to Survey of Customer Concerns," *PC World online*, 29 November 2005.

Gross, Grant. "Security Expert: More Sophisticated Net Attacks Likely," *PC World Online*, 29 November 2005.

Gross, Grant. "Call for Homeland security Cybersecurity Improvements: Recovery Plan Needed for Widespread Attack on the Internet, Senate Committee Told," *PC World Online*, 19 July 2005.

Gross, Grant. "Air force will Guard Cyberspace: New Mission Space Stakes First Claim by Military Service, *PC World Online*, 9 December 2005.

Hayes, Richard and Gary Wheatley, "Information Warfare and Deterrence." *Strategic Forum* 87, October 1996.

Holdridge, KipR, and MissouriStateUniversity.Dept.ofDefenseandStrategicStudies. "The Utility of Cyberattack as a Tool for Military Operations the Case of China Vs. the United States." 2006.

Liang, Qiao and Wang Xiangsui, *Unrestricted Warfare*, (Beijing: PLA Literature and Arts Publishing House, February 1999), p. 166.

Mandruaud, Issabelle. "France Targeted by Chinese Hackers," *World News Connection*, 10 September 2007.

Libicki, Martin. *Defending Cyberspace and other Metaphors* (Washington D.C.: National Defense University Press, 1997), 9.

Libicki, Martin. *The future of Information Security* (Washington D.C.: National

Marquand, Robert. "Chinese Build high-tech Army Within an Army," *Christian Science Monitor online*, 17 November 2005.

McMillan, Robert. "Cyberthreats: Fluid and Far Reaching," *PC World Online*, 15 February 2006. Defense University Press, 1981).

Rollins, John and Clay Wilson, Terrorist Capabilities for Cyberattack: Overview and Policy Issues. (Washington D.C.: Congressional Research Service, Division of Foreign Affairs, Defense and Trade, 20 October 2005. P. 3, RL33123.

Pasternak, Douglas and Bruce B. Auster. "Terrorism at the Touch of a Keyboard." U.S.News & World Report 125, no. 2; 2 (07/13, 1998): 37 (accessed 11/1/2007).

Dupuy, Trevor . The Chinese Civil War
(New York: Franklin Watts Inc, 1969), 4.

SANDBERG, JARED. "Holes in the Net. (Cover Story)." Newsweek 135, no. 8; 8 (02/21, 2000): 46 (accessed 11/1/2007).

Shea, Dana. Critical Infrastructure: Control Systems and the Terrorist Threat (Washington D.C.: Congressional Research Service, Division of Resources, Science, and Industry, 20 January 2004), P. 1, RL31534.

Thomas, Timothy. Like Adding Wings to the Tiger: Chinese Information Theory and Practice (Fort Leavenworth, KS: Foreign Military Studies, 2003).

Thomas, Timothy. "Chinese and American Network Warfare," *Joint Forces Quarterly* 38 (Summer 2005), p. 77.

Vistica, Gregory L. and Evan Thomas. "The Secret Hacker Wars." Newsweek 131, no. 22; 22 (06/01, 1998): 60 (accessed 11/1/2007).