CYBER WARFARE: CHINA‘S STRATEGY TO DOMINATE IN CYBER SPACE

A thesis presented to the Faculty of the U.S. Army
Command and General Staff College in partial
fulfillment of the requirements for the
degree

MASTER OF MILITARY ART AND SCIENCE
Strategy

by

JOHN OAKLEY, MAJOR, USA
B.S., University of Minnesota, St. Paul, Minnesota, 1993

Fort Leavenworth, Kansas
2011-01

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 this 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 Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

1. REPORT DATE *(DD-MM-YYYY)* 10-06-2011	**2. REPORT TYPE** Master‘s Thesis	**3. DATES COVERED** *(From - To)* AUG 2010 – JUN 2011

4. TITLE AND SUBTITLE Cyber Warfare: China‘s Strategy to Dominate in Cyber Space	**5a. CONTRACT NUMBER** **5b. GRANT NUMBER** **5c. PROGRAM ELEMENT NUMBER**
6. AUTHOR(S) MAJ John Oakley	**5d. PROJECT NUMBER** **5e. TASK NUMBER** **5f. WORK UNIT NUMBER**
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) U.S. Army Command and General Staff College ATTN: ATZL-SWD-GD Fort Leavenworth, KS 66027-2301	**8. PERFORMING ORG REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)	**10. SPONSOR/MONITOR’S ACRONYM(S)** **11. SPONSOR/MONITOR’S REPORT NUMBER(S)**

12. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for Public Release; Distribution is Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

China‘s INEW doctrine combining network attack with electronic warfare supports the use of cyber warfare in future conflict. The IW militia unit organization provides each Chinese military region commander with unique network attack, exploitation, and defense capabilities. IW unit training focuses on improving network attack skills during military exercises. The integration of the IW militia units with commercial technology companies provides infrastructure and technical support enabling the units to conduct operations. The IW units gather intelligence on an adversary‘s networks identifying critical nodes and security weaknesses. Armed with this intelligence, these units are capable of conducting network attack to disrupt or destroy the identified critical nodes of an enemy‘s C4ISR assets allowing China to use military force in a local war. In an effort to regain its former status, China pursues the strategic goal of reunification of its claimed sovereign territories and lands using economic influence as the primary means but will resort to military force if necessary. Recent cyber activities attributed to China suggest that network exploitation is currently underway and providing military, political, and economic information to the CCP. Domestically and internationally, China views Taiwan and the United States respectively as the major threats to the CCP.

15. SUBJECT TERMS
China, Strategy, Cyber Warfare, Cyber Space, Information Warfare, Electronic Warfare

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. PHONE NUMBER** *(include area code)*
(U)	(U)	(U)	(U)	99	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

MASTER OF MILITARY ART AND SCIENCE

THESIS APPROVAL PAGE

Name of Candidate: MAJ John T. Oakley

Thesis Title: Cyber Warfare: China's Strategy to Dominate Cyber Space

Approved by:

____, Thesis Committee Chair
Scott A. Porter, M.Ed.

____, Member
David A. Anderson, DBA

____, Member
Stephen Melton, M.A.

____, Member
Timothy L. Thomas, M.A.

Accepted this 10th day of June 2011 by:

____, Director, Graduate Degree Programs
Robert F. Baumann, Ph.D.

The opinions and conclusions expressed herein are those of the student author and do not necessarily represent the views of the U.S. Army Command and General Staff College or any other governmental agency. (References to this study should include the foregoing statement.)

ABSTRACT

CYBER WARFARE: CHINA‘S STRATEGY TO DOMINATE CYBER SPACE, by MAJ John T. Oakley, 99 pages

China‘s INEW doctrine combining network attack with electronic warfare supports the use of cyber warfare in future conflict. The IW militia unit organization provides each Chinese military region commander with unique network attack, exploitation, and defense capabilities. IW unit training focuses on improving network attack skills during military exercises. The integration of the IW militia units with commercial technology companies provides infrastructure and technical support enabling the units to conduct operations. The IW units gather intelligence on an adversary‘s networks identifying critical nodes and security weaknesses. Armed with this intelligence, these units are capable of conducting network attack to disrupt or destroy the identified critical nodes of an enemy‘s C4ISR assets allowing China to use military force in a local war. In an effort to regain its former status, China pursues the strategic goal of reunification of its claimed sovereign territories and lands using economic influence as the primary means but will resort to military force if necessary. Recent cyber activities attributed to China suggest that network exploitation is currently underway and providing military, political, and economic information to the CCP. Domestically and internationally, China views Taiwan and the United States respectively as the major threats to the CCP.

ACKNOWLEDGMENTS

I wish to acknowledge the members of my committee for their direction and assistance provided in the writing of this thesis. Without their diligent efforts this work would not have been possible. I wish to thank Mr. Scott Porter for his efforts in keeping me on track to complete the work on time and in organizing the committee meetings, oral comprehensive boards, and the thesis defense. I also wish to acknowledge the hours spent in mentoring me throughout the year as my faculty advisor.

I wish to recognize the guidance provided by Dr. David Anderson in helping me formulate the research question and methodology. Our conversations greatly assisted me in understanding how to formulate my plan in approaching this subject and for that I am grateful. Mr. Stephen Melton provided me the idea for this paper and was instrumental in helping me to focus on developing the topic of research. Lastly, to Mr. Timothy Thomas who provided extensive background on this subject and motivated me in taking a different approach in my research. To each of these men I am forever thankful for their knowledge and diligence in helping me throughout the process of writing this thesis.

I would be remiss if I failed to acknowledge the sacrifices of my family during this year of study. To my daughters who have lived with the absence of a father in the military, I can never bring back the lost time but I always carried your —heart” with me. To my wife I owe the world. Partners in life and travellers together as we make the journey, side by side, in love.

TABLE OF CONTENTS

ACRONYM

FM	Field Manual
IW	Information Warfare
JP	Joint Publication
PLA	People‘s Liberation Army
PLC	Programmable Logic Controller
PRC	People‘s Republic of China
U.S.	United States

ILLUSTRATIONS

Page

CHAPTER 1

INTRODUCTION

> In a possible future war, the rules of victory will make extremely harsh demands on the victor. Not only will they, as in the past, demand that one know thoroughly all the ingenious ways to contest for victory on the battlefield. Even more so, they will impose demands which will mean that most of the warriors will be inadequately prepared, or will feel as though they are in the dark: the war will be fought and won in a war beyond the battlefield; the struggle for victory will take place on a battlefield beyond the battlefield.
>
> — Qiao Liang and Wang Xiangsui, *Unrestricted Warfare*

Background

Cyber warfare is one of the newest threats to emerge in the contemporary operating environment. As such, nation-states are reevaluating current strategies and factoring in the best method of employing this capability against their enemies while simultaneously protecting their own networks from attack. Advances in technology create a rapidly evolving threat of technologically adept adversaries from individual computer hackers to criminals to terrorist organizations to nation-state organized and trained cyber warfare units.

Government, finance, energy, and military networks rely on connections to the Internet to perform daily functions. These connections provide hackers access points into the networks where they can steal trade secrets, disable websites, or infect computers with malicious software. President Barack Obama identified cyberattacks as —one of the most serious economic and national security challenges we face as a nation."[1] In the last decade, the frequency of reported incidents of malicious activity on Department of Defense networks alone increased fifty fold.[2] The White House, the United States House of Representatives, the Department of State, the National Aeronautics and Space Administration, the Oak Ridge National Laboratory, and the United States Naval War College experienced malicious cyber activity as well.[3]

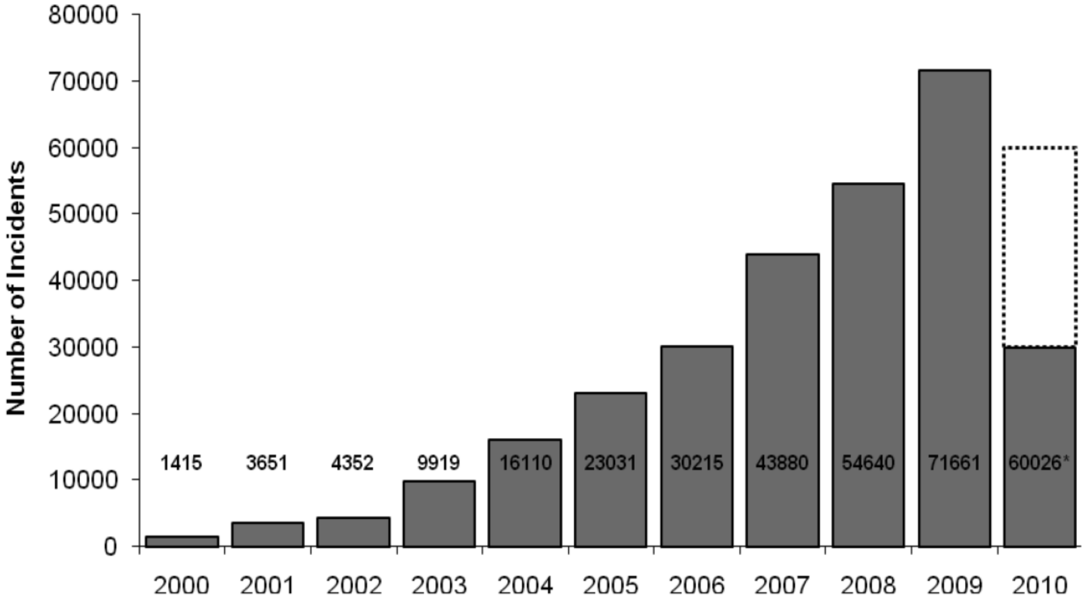

Figure 1. Department of Defense Reported Incidents of Malicious Cyber Activity, 2000-2009, with Projections for 2010

Source: Daniel M. Slane, Chairman, *2010 Report to Congress of the U.S.-China Economic and Security Review Commission* (Washington, DC: Government Printing Office, November 2010), 237.

Computer hacker groups from China and the United States initiated distributed denial of service attacks and web site vandalism against government and private sites in April 2001 following a mid-air collision between a United States Navy EP-3 reconnaissance plane and a Chinese People‘s Liberation Army Navy F-8 fighter over the South China Sea.[4] The attacks lasted for a period of eight days as hackers, sparked by nationalism sought to deface and overwhelm websites.

Cyber incursions into the United States electrical power grid and other key infrastructure systems took place in April 2009. Experts suspect that China or Russia played a part in an alleged attempt to map the power system and its key control systems, though forensic analysis was unable to verify this. Computer networks control the flow of electrical power efficiently around the country through a series of supervisory control and data acquisition systems, digital control systems, and programmable logic controllers. Investigators detected no immediate damage or threat but found software tools left behind that could allow future access to the network, thereby creating the potential to destroy or manipulate the systems.[5]

The capability of other nations or actors to conduct cyber warfare is rapidly increasing. Similarly, the potential damage or the severity of the threat and its consequences is also dramatically increasing. Until recently, cyberattacks focused on obtaining data or causing systems to crash. Discovered in July 2010, the Stuxnet worm heralds an entirely new and sinister threat that goes beyond vandalism of a website or stopping the flow of email traffic. Stuxnet is software known as a worm, which means that it infects, or attacks computer systems, replicates itself, and then passes itself along to other computers to begin the process again. Unlike computer viruses, computer worms do not rely on the user to spread from one computer to another. The real danger of the Stuxnet worm lies in its unique potential to cause the physical destruction of infected systems by overriding commands from human operators.

The Stuxnet worm specifically targets Siemens programmable logic controllers and replaces critical portions of the software source code preventing digital control systems or operators from properly managing the controller. Used throughout the world, programmable logic controllers maintain process control of systems like the United States power grid. In one specific case, Stuxnet infected critical operational control systems in Iran‘s Bushehr nuclear power plant just weeks before the plant came online.[6] Mahmoud Jafari, the plant manager at the Bushehr facility, acknowledged that Stuxnet infected several computers but that ―tihas not caused any damage to major systems of the plant."[7] In the case of the Bushehr facility, infected controllers have the potential to shut down critical reactor functions resulting in a reactor core meltdown and potential explosion. It is not clear who developed Stuxnet or if there was an intended target but due to its level of sophistication, security analysts believe that it was state sponsored.[8]

In August 2008, the world witnessed one of the first uses of cyber space and cyber warfare as a means to control information on the battlefield. Distributed denial of service attacks, presumably from Russia, hit several Georgian government websites simultaneously. These attacks targeted and effectively shut down the websites of the Georgian President, the Ministry of Defense, and the Ministry of Foreign Affairs. This attack coincided with the attack of Russian ground forces as they moved into South Ossetia.[9] While the cyberattacks played no significant role in the overall outcome, they did signal a new threat on today‘s battlefield.

Malicious types of software like Stuxnet or coordinated distributed denial of service attacks as seen in Georgia, are quickly transforming cyber space from a future threat to the newest frontline of warfare. In response to this growing threat, Secretary of Defense Robert Gates instructed United States Strategic Command to establish a new functional command known as Cyber Command. Cyber Command reached full operating capability in November 2010.[10] Cyber Command ―plans, coordinates, integrates, synchronizes, and conducts activities to: direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full-spectrum military cyber space operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyber space, and deny the same to our adversaries."[11]

The United States is not the only country to recognize the possibilities or the threat afforded in cyber space. China too recognizes the need to secure networks and prevent interruption or damage from enemy attacks. Major General Dai Qingmin of the PLA is a longtime supporter and developer of information warfare doctrine and theories.

As early as 1999, Dai discussed ―thecombined use of network and electronic warfare to seize control of the electromagnetic spectrum."[12] As the author of China‗s integrated network electronic warfare strategy, Dai advocates for the combination of electronic warfare coupled with computer network operations against enemy command, control, communications, computers, intelligence, surveillance, and reconnaissance systems as a means to disrupt information collection during combat operations.[13] Shortly after the publication of his book, *On Information Warfare*, Dai was promoted to head the Communications Department and eventually to lead the 4th Department of the Chinese General Staff.[14]

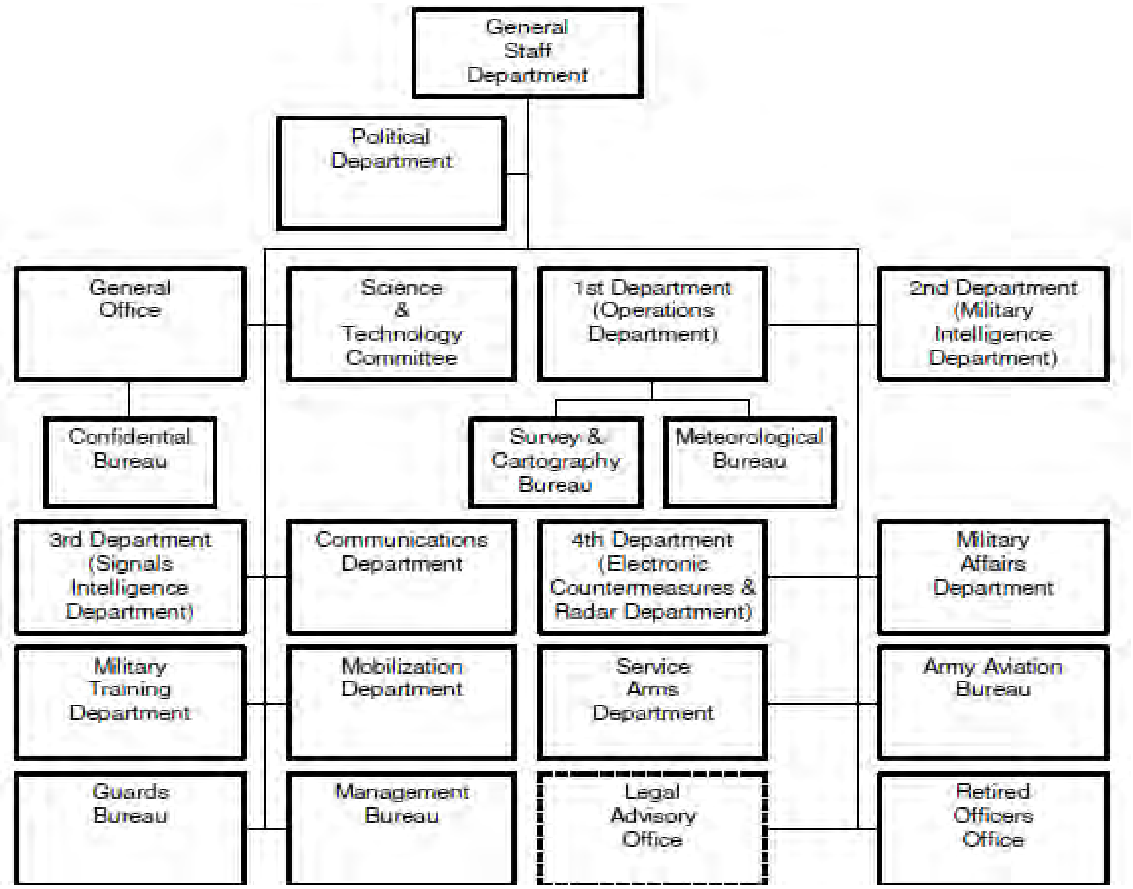
General Staff Department
Political Department
General Office
Science & Technology Committee
1st Department (Operations Department)
2nd Department (Military Intelligence Department)
Confidential Bureau
Survey & Cartography Bureau
Meteorological Bureau
3rd Department (Signals Intelligence Department)
Communications Department
4th Department (Electronic Countermeasures & Radar Department)
Military Affairs Department
Military Training Department
Mobilization Department
Service Arms Department
Army Aviation Bureau
Guards Bureau
Management Bureau
Legal Advisory Office
Retired Officers Office

Figure 2. General Staff Department of the People‘s Liberation Army
Source: Bryan Krekel, *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation* (McLean, VA: Northrup Grumman Corporation, 9 October, 2009), 31. Reprinted from David Finkelstein, —The General Staff Department of the Chinese People‘s Liberation Army: Organization, Roles, and Missions," in *The People's Liberation Army as Organization Reference Volume v1.0*, ed. James C. Mulvenon and Andrew N. D. Yang (Santa Monica CA: RAND Corporation, 2002).

Similar to the United States Cyber Command, China‘s 3rd and 4th Departments of the General Staff Department share computer network operation responsibility in addition to more traditional information and electronic warfare (figure 2). The 3rd Department is responsible for signals intelligence, computer network defense, and computer network exploitation. The 4th Department is responsible for electronic countermeasures and radar as well as computer network attack.

Assumptions

There are two basic assumptions used as the basis for this study. The first assumption is that the benefits offered by globalization and the networking and sharing of information and ideas in cyber space far outweigh the inherent risks associated with such connectivity and will continue to dominate the way that individuals and nations will interact with each other. Globalization coupled with the Internet represents a major shift in the way people communicate and interact. As *New York Times* columnist Thomas Freidman asserted, ―Globalization, at least in my view, is not a trend. [I]t is actually the international system that replaced the Cold War system and like the Cold War system, the globalization system has its own rules, logic, pressures, incentives, and moving parts that will and do affect everyone's company, country, community."[15] The Internet speeds globalization along by saving time, eliminating distances, and opening new access to information that previously was the purview of nations and governments or a few select individuals. The ability for all people to participate and interact on a worldwide stage has had a profound affect. The democratization of information changes people's lives.[16]

The second assumption is that the use of cyber space for malicious purposes will continue to exist. Regardless of the adversary, whether hacker groups, criminals, or states, the malicious exploitation of computer vulnerabilities has existed since 1984 with the discovery of the very first computer virus generated outside of a laboratory. Since then, viruses, worms, and Trojan horses of all types continue to become more sophisticated and insidious resulting in damages or lost revenue estimated in the billions of dollars worldwide.

Definitions

Cyber space presents new challenges to governments and militaries. To understand the environment better, it is important that definitions clearly establish the description of the cyber environment and the different ways it is used. Terms like computer network attack or computer network exploitation are useful only when agreed upon standards are developed and appropriate definitions applied. Knowing what constitutes an act of cyber warfare or more importantly, how others, particularly the Chinese, define cyber warfare is critical in understanding this subject.

Currently neither the United States nor international law has a legal or doctrinal definition of cyber warfare.[17] The Constitution of the United States Article 1, section 8, specifies that only Congress can declare war. Additionally, the War Powers Resolution as codified in 50 U.S.C. 1541 says that the President‘s powers as Commander in Chief are pursuant to a declaration of war, with specific authorization from Congress, or in a national emergency created by an attack upon the United States. Lacking further clarification from these sources, a different approach to defining cyber warfare is possible by defining its subcomponents.

Definitions taken from Field Manual 1-02, *Operational Terms and Graphics*, Field Manual 3-13, *Information Operations*, and Joint Publication 3-13, *Information Operations* focus on computer network operations or its subcomponents. Computer network operations are comprised of computer network attack, computer network defense, and computer network exploitation. Field Manual 3-13 defines computer network operations as ―Computer network attack, computer network defense, and related computer network exploitation enabling operations."[18] Joint Publication 3-13 defines computer network attack as ―actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.”[19] This definition is identical in Field Manual 1-02 and Field Manual 3-13.

Computer network defense is the ―actions taken through the use of computer networks to protect, monitor, analyze, detect, and respond to unauthorized activity within Department of Defense information systems and computer networks”[20] as defined in Joint Publication 3-13. Field Manual 1-02 and Field Manual 3-13 present a slightly different version that addresses computer network defense as ―measures to protect and defend information, computers, and networks from disruption, denial, degradation, or destruction.”[21]

Lastly, all three publications define computer network exploitation as ―enabling operations and intelligence collection to gather data from target or adversary automated information systems or networks.”[22] Comparing United States definitions of computer network operations, computer network attack, and computer network defense to China‘s definitions reveals similar definitions with one exception. The Chinese discuss the concept of computer network reconnaissance rather than computer network exploitation. The substitution of reconnaissance for exploitation might suggest a difference in thought, but the two definitions have virtually no difference and align well together. This study will use the definition of computer network operations and considers that definition synonymous with the term cyber warfare.

As mentioned earlier, Dai developed a unique concept called integrated network electronic warfare. INEW is the combined use of computer network operations and electronic warfare against an adversary‘s key information networks, command and control systems, and reconnaissance assets.[23]

Scope

The principle aim of this study is to determine the significance of cyber warfare in China‘s national strategy. From a U.S. perspective, strategy is the overarching concept that links ends, ways, and means and this study will use this approach to determine China‘s strategy to dominate cyber space. The scope of this study does not consider all aspects of China‘s national strategy but rather focuses on cyber warfare in an effort to determine the logic and reasoning behind China‘s strategy.

The goal is to understand what makes the strategy uniquely Chinese or as stated by the Chinese, a strategy with Chinese characteristics. This study focuses on cyber warfare capabilities, official policy, China‘s cyber activities, culture and history, and finally threats to China. It is impossible to incorporate a Chinese perspective without understanding culture. Culture, history, and even politics integrate into the national psyche and manifest themselves in unique and sometimes nationalistic perceptions in terms of values, rituals, practices, and symbols. While the citizens of a nation do not actively reflect on historical events in making daily decisions, there remains an influence of those events on a subconscious level. Subtle though they may be, these influences accumulate over time and pass from generation to generation in the form of values, ideas, and practices. The Chinese Opium Wars have no direct correlation to cyber warfare, but the idea that the humiliation of China by foreign intervention during the wars does influence perception and consequently influences strategy. Understanding these factors provides insight into what makes China‘s strategy inherently Chinese.

Culture and history play an important role in defining a Chinese strategy. However, it is also important to understand China's current capabilities because a strategy is only effective if the means to execute it are available. In this respect, China has created specialized cyber warfare units and developed a doctrine of fighting under informationized conditions.[24] The discussion of capabilities is not limited strictly to cyber warfare capabilities. No nation has the resources to develop a capability for every possible threat. Strategies must maximize the strengths of existing capabilities while simultaneously minimizing the weaknesses. Therefore, it is important to understand how combinations of capabilities achieve the strategic ends while simultaneously countering vulnerabilities and preserving overall strength. An example might be that the cyber warfare unit is strong in attacking an enemy without risking total war but is weak in its capability to destroy an adversary. Alternatively, the capability of conducting a nuclear attack is strong in destroying an enemy but is weak in its ability to prevent retaliation. Used in combination, these two capabilities complement each other by compensating for weakness without sacrificing overall strength.

The most outward and visible manifestation of a strategy is the direct action itself and the consequences. Linked with the capability or means used in perpetrating the action, the action itself offers insight to a particular strategy. While this type of analysis leads to inductive rather than deductive reasoning and is susceptible to bias, the result provides plausible solutions in determining a strategy. Knowing the origin of a cyber attack, the method used in conducting the attack, and the intended target provide information to induce the intent of the attack and from there a possible strategy.

Developing an effective strategy first requires knowing the desired outcome and then understanding the possible threats that prevent achieving the outcome. Without this critical link, a strategy is ineffective and wastes effort. Understanding strategy development and determining the threats facing China, provides insight about China‘s strategic ends. China faces many threats but it is not important to study each in detail rather only the threats with the greatest potential to prevent China from achieving its goals. The difficulty lays in determining which threats have, or do not have, the most influence in developing a strategy. An example is the ability of the U.S. to prevent China from achieving its goals is much greater than the ability of a third world country to do the same. Therefore, the U.S. poses a greater threat and thus has more influence on China‘s strategy development. This example is easy to analyze and assess but threat analysis is not always so obvious. The challenge lays in trying to determine the influence of disparate threats.

Lastly, it is important to know what China says about their strategy. Many are skeptical of China‘s publicly released information and their specified intentions. This public skepticism is a reflection of China‘s lack of transparency and their tight control over information offers little to the international community to change this opinion. However, this does not wholly invalidate what China does release through the media. The best deception plan has at least some truth in order to make the deception more plausible.

The primary question of this study is to understand the significance of cyber warfare in China‘s national strategy. Developing an answer to this question requires answering secondary questions on the five topics mentioned earlier. First, what are the cyber warfare capabilities or means that execute China‘s national strategy? This leads to asking what resources and training are required to develop this cyber warfare capability? Is China pursing a doctrine that supports the use of cyber warfare? What is a possible organizational structure that reflects the fusion of doctrine, resources, and training? What domestic and cyber policies support the pursuit of China‘s national strategy? What recent cyber domain activities confirm or deny the possible ends and ways of China‘s national strategy? How do Chinese history, culture, and politics influence the development of possible ends and ways? Finally, what is China‘s analysis of the security situation? The answers to these questions show that cyber warfare is a significant component of China‘s national strategy. In particular, China‘s cyber capabilities support the ends of their national strategy by exploiting America‘s heavy reliance on networked information systems through deception, deterrence, and reconnaissance.

China views the world from a significantly different perspective than the U.S. It is this view that influences the development of a strategy with Chinese characteristics. Analysis of what China views as the current threat and an assessment of their capabilities form the basis for the development of a strategy. Chinese culture, history, and politics greatly influence China‘s perception of the world and help define a strategy with Chinese characteristics. China‘s recent actions are not always in line with their current public policies and statements. Understanding these five factors in detail and their specific influence on strategy, reveals China‘s likely strategy and the use of comprehensive national power to achieve domination in cyber space.

Limitations

Unlike the United States where unclassified strategic documents are available for general consumption, China strictly limits the amount and type of information released regarding its national or military strategy. China‘s 2008 National Defense White Paper is the most recent official document released. Unlike the United States where dissenting or opposing views are part of the daily discourse, the Chinese Communist Party controls all information and scholars are limited to the few pieces of available information when conducting research. This leads to a significant overlap of the same material used as the source documents in reports, papers, and articles. The limitation is that the basis for much of the research comes from the same source documents and its subsequent conclusions reflect the same mindset.

A second limitation due to the lack of available documents is the quantitative ability to ascertain China‘s strategic design. This is not to say that material such as the 2010 National Defense Paper is inherently worthless, rather it does offer a glimpse into the Chinese strategic approach in the same way that the United States‘ National Security Strategy offers an understanding of American thinking. However, the forensic study of additional writings from ancient Chinese military strategists, philosophers, or its recent leaders may offer insight and answers otherwise unavailable.

Delimitations

The idea of developing a comprehensive understanding of China‘s overall national strategy is an overwhelming task. It is beyond the scope of this paper to comprehend a strategy regarding the plethora of issues currently facing China such as the environment, nuclear proliferation, economic development, or Taiwan. Instead, the research focused specifically on the strategic approach to IW by the PLA and in particular developing a knowledge based on the PLAs cyber warfare capability and the domestic threat and the perceived threat of the United States. China‘s concept of national power incorporates diplomatic, informational, military, and economic aspects as well as international prestige, domestic cohesiveness, and cultural influence.[25]

Due to the inability of this author to read Chinese, translations of the original documents by other sources substituted for the source document. While there is some discrepancy between the original and translated versions, the translations are widely accepted by academics. Lastly, this study uses only open source documents for the basis of research. The use of classified material would likely offer a more definitive analysis but would also restrict the available audience. It is not clear that classified material significantly improves the overall study and offsets the dissemination restrictions.

Several areas of IW that this study does not research but require further consideration are information anti-access and area denial strategies, space operations, and INEW. Of particular interest and integrated with cyber warfare is industrial cyber espionage. The subject of cyber espionage as part of computer network operations offers a full range of topics by itself. In the course of research for this study, industrial cyber espionage is a central theme in many of the writings and practical examples involving China are readily available. To illustrate this point East Asia and the Pacific were the most active regions in 2009 in the attempted collection of United States defense technologies. Additionally, 17 percent of the attempted collections involved cyber collection techniques.[26]

Importance

China is quickly developing into the world‘s second superpower, replacing the former Soviet Union as America‘s primary rival for global influence. Projections show China will rival the United States economically and militarily by 2030. As China‘s economic, industrial, and military strength grows, it must consider what role cyber warfare will play in its ascendency in the world. In the realm of cyber space, activities occurring on the opposite side of the globe will now affect every nation. China is no exception and it too has experienced the negative effects that interconnectivity brings. Interconnectivity offers great advantages and opportunities never before attainable, but it also presents a unique set of problems. Nations must develop strategies that exploit their adversary‗s vulnerabilities while simultaneously reducing their own risk.

Unlike traditional warfare that moves at speeds measured in days or hours, cyber warfare happens in milliseconds. At such speeds, it is imperative that any strategy is comprehensive. Unfortunately, software programmers are limited to developing defensive measures based on the current or known threat. New threats, however, exploit flaws that have no current defense. This gap confers a significant advantage to the attacker. Therefore, a purely defensive strategy in cyber warfare does not ensure adequate protection and yields the initiative. A strategy designed around an offensive approach with defensive capability is the most logical.

Lastly, it is important to make a determination of Chinese strategy as viewed from the Chinese perspective rather than the perspective of the U.S. Understanding the Chinese viewpoint and in particular their specific approach to developing strategy, is required to obtain a more accurate picture. Doing so will allow for a more thorough understanding of the Chinese strategy itself thereby allowing the United States to develop a counterstrategy that targets Chinese vulnerabilities with American strengths.

[1] Barak Obama, ―Remarks by the President on Securing Our Nation‗s Cyber Infrastructure" (Washington, DC: The White House 29 May 2009), http://www.white

house.gov/ the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/ (accessed 3 March 2011).

[2] Daniel M. Slane, Chairman. *2010 Report to Congress of the U.S.-China Economic and Security Review Commission* (Washington, DC: Government Printing Office, 2010), 237.

[3] Bryan Krekel, —Capability of the People‘s Republic of China to Conduct Cyber Warfare and Computer Network Exploitation," (McLean, VA: RAND Corporation, 9 October 2009), 68-74.

[4] Krekel, 69.

[5] Siobhan Gorman, —Electricity Grid in U.S. Penetrated by Spies," *Wall Street Journal*, 8 April 2009, http://online.wsj.com/article/SB123914805204099085.html (accessed 22 February 2011).

[6] Robert McMillan, —Was Stuxnet Built to Attack Iran‘s Nuclear Program?" *PCWorld* (21 September, 2010), http://www.pcworld.com/businesscenter/article/205827/ was_stuxnet_built_to_attack_irans_nuclear_program.html (accessed 30 March 2011).

[7] Associated Press, —Computer Worm Affects Computers at Iran‘s First Nuclear Power Station," *Fox News*, 26 September 2010, http://www.foxnews.com/world/ 2010/09/26/worm-affects-computers-irans-nuclear-power-station/ (accessed 10 December 2010).

[8] McMillan.

[9] Tony Skinner, —War and PC: Cyberwarfare," *Jane's Defence Weekly* (19 September 2008).

[10] Elanor Keymer, —Analysis: Is the Threat of Cyber Attack Overblown?" *Jane's Defence Weekly* (20 January 2011).

[11] United States Strategic Command, —Fact Sheets," http://www.stratcom.mil/ factsheets/Cyber_Command/ (accessed 15 January 2011).

[12] Krekel, 14.

[13] Ibid., 13.

[14] Krekel, 15; Timothy L. Thomas, *Decoding the Virtual Dragon* (Fort Leavenworth, KS: Foreign Military Studies Office, 2007), 117.

[15] Thomas Friedman, —National Strategies and Capabilities for a Changing World: Globalization and National Security," in C100, *Foundations*, Department of Command and Leadership (Fort Leavenworth, KS: Government Printing Office, 2010), 82.

[16] Friedman, 82.

[17] Jonathan A. Ophardt, ―Cyberwarfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow‘s Battlefield,” *Duke Law and Technology Review* (Durham, NC: February 2010), http://www.law.duke.edu/journals/dltr /articles/2010dltr003.html#B19 (accessed 26 April 2011); The Economist, ―Marching Off to Cyberwar,” *The Economist* (4 December 2008), http://www.economist.com/ node/12673385?story_id=12673385 (accessed 26 April 2011).

[18] U.S. Army Training and Doctrine Command (TRADOC), Field Manual (FM) 3-13, *Information Operations: Doctrine, Tactics, Techniques, and Procedures* (Washington, DC: Government Printing Office, November 2003), Glossary-5.

[19] Chairman of the Joint Chiefs of Staff (CJCS), Joint Publication (JP) 3-13, *Information Operations* (Washington, DC: Government Printing Office, February 2006), GL-5; TRADOC, FM 3-13, Glossary-5; U.S. Army Training and Doctrine Command (TRADOC), Field Manual (FM) 1-02, *Operational Terms and Graphics* (Washington, DC: Government Printing Office, September 2004), 1-42.

[20] CJCS, JP 3-13, GL-5.

[21] TRADOC, FM 3-13, Glossary-5; TRADOC, FM 1-02, 1-42.

[22] CJCS, JP 3-13, GL-6; TRADOC, FM 3-13, Glossary-5; TRADOC, FM 1-02, 1-42.

[23] Krekel, 13.

[24] Ibid., 10.

[25] Office of the Secretary of Defense, *Annual Report to Congress: Military Power of the People's Republic of China 2007* (Washington, DC: Government Printing Office, 2007), 6.

[26] Thomas Badoud, Frank Carapezza, Hilary Clark, Kathryn Cubbon, Tim Deerr, Sara DeWitz, Chris Fraser, Jessica Rocha, James Stanley, Jon Stevenson, and Laresa Walter, ―Targeting U.S. Technologies: A Trend Analysis of Reporting from Defense Industry, 2010” (Washington, DC: Government Printing Office, 2010), 24.

CHAPTER 2

LITERATURE REVIEW

> Innovations and creative thinking, in the view of the PLA, are the keys to victory in future war. This requires escaping from the grasp of mechanized thought and finding new and innovative ways to implement informatized thinking. Innovations involve finding new ways to apply ancient stratagems to information age developments. In a certain sense, a new mode of thinking is an asymmetric answer to a competitor with technological prowess but who has failed to apply these advances to their fullest.
>
> — Timothy Thomas, *The Dragon's Quantum Leap*

Overview

While there are many articles, reports, and papers pertaining to China and cyber warfare this study will focus on three principle types of sources. The first type of work comes directly from the Chinese government, most notably the 2010 National Defense White Paper, but includes other works by Chinese military leaders. The second type is United States Government sources or work specifically commissioned by the United States Government. A majority of this work comes from a Northrup Grumman report provided to the U.S.-China Economic and Security Review Commission. The third body of work comes from independent scholars, journalists, and analysts. Each of these sources provides a slightly different view of the subject matter but with little variation considering China's capabilities. The general viewpoint outside of China tends to consider the relationship with China as either outright adversarial or optimistically cautious.

The majority of the works discussed in this chapter come from the second type of literature, namely United States Government sources. The reports are thorough and comprehensive such that the material covered extends well beyond the limits of cyber warfare; however, this also allows a more detailed examination of possible trends and linkages between topics and therefore a more comprehensive view of Chinese strategy. While the official reports compile the testimony or reports from several different sources, the major contributor to the knowledge on China‘s information warfare capabilities and strategy comes from the Northrup Grumman Report.

The body of literature covers a wide range of topics not exclusively related to cyber warfare. The subject of China is so complex that it is virtually impossible to discuss one topic without addressing other issues. The result is literature that must address multiple topics in order for the reader to get a true appreciation of the complexity of the issue. In this regard, the literature used in this study is no different. As a result, this study devised five general categories based on the principles of strategy development and grouped the content from the literature into these categories. In doing so, this highlights the interconnections between the various topics discussed in the literature.

This chapter has five main sections: capabilities, policy, activities, culture, and threat, in an effort to address each of the questions presented in chapter one. This study parsed the sources individually into the general categories in order to find commonality relating the works. While each source does not address every category, most sources address at least two.

The section on China‘s capabilities discusses China‘s current known capabilities such as specialized cyber warfare units and technologies. The next section focuses on China‘s official stance regarding cyber warfare and their current strategy. Following this is a section highlighting China‘s recent actions with a discussion on the differences between their actions and rhetoric. The section on China‘s culture focuses on the historical, political, and cultural characteristics of China and the meaning of a strategy with Chinese characteristics. The final section focuses on the internal and external threats to China.

Capabilities

The PLAs General Staff Department divides computer network operations between the 3rd and 4th departments. The 3rd Department which heads the signals intelligence collection effort has the responsibility for overseeing computer network defense and computer network exploitation.[1] As mentioned previously, the 4th Department is responsible for computer network attack.[2]

Starting in the late 1990s or early 2000s, the PLA began the process of creating IW militia units comprised of academics, commercial information technology experts, and possibly former computer hackers. Integrated into commercial information technology firms, these units have direct access to technical expertise, the latest hardware and infrastructure, and sophisticated software design.[3] Qiao Liang and Wang Xiangsui note in *Unrestricted Warfare* that —a pasty-faced scholar wearing thick eyeglasses is better suited to be a modern soldier," and while this is clearly a stereotype, this does reflect the idea that cyber warfare requires more brains than brawn.

By 2003, the Chinese Academy of Military Science published writings establishing four IW militia units as a proof of concept.[4] Centered in China‘s Guangdong province, home to the heaviest concentration of commercial information technology companies in China, the militia units recruited personnel with computer network expertise, advanced degrees, and educational experience outside of China.[5] The units focused research on —launching hacker attacks, propagating viruses, jamming information channels, and disrupting nodes of enemy networks."[6] In 2006, the Academy of Military Science explicitly directed the PLA to establish IW militia units.[7]

Recently in March 2008, the newest IW unit organized in the Ningxia Province. Reporting the event on the county website revealed the mission of the unit, its size, and organization. The website stated the new unit would, —In peacetime, extensively collect information from adversary networks and establish databases of adversary network data…In wartime, attack adversary network systems, and resist enemy network attacks."[8] The posting continues, saying that the unit is comprised of approximately 80 personnel and organized into three detachments. The detachments specialize in the full range of computer network operations.[9] The exact number of IW units or the level of their capabilities is currently unknown.

In addition to the PLA formed IW militia units, six technical reconnaissance bureaus formed throughout the country. The full purpose of these bureaus remains unknown but along with traditional signals intelligence collection it appears that computer network exploitation is one of their missions. The Chinese Communist Party media outlet recognized that the First TRB received commendations —for substantial achievements in informatization building."[10] In 2002, a similar report noted that the Third TRB —received its fifth consecutive award for outstanding research in IW theories,"[11] implying that the technical reconnaissance bureaus existed as early as 1997.[12]

Computer hackers are the last capability available to China. In 2007, *Time* reported on a computer hacker, Tan Dailin, also known by the screen name of Withered Rose. Tan, who was a student at Sichuan University of Science and Engineering, is the leader of the Network Crack Program Hacker group. Founded in 2004, the Network Crack Program Hacker group earned its reputation by hacking into other hacker group websites and by July 2005 drew the attention of the Sichuan Military Command Communication Department. The department invited Tan‘s group to participate in a computer hacker competition sponsored by the Chengdu Military Command. Tan‘s group won the competition and then, —had a month of intense training organized by the provincial military command, simulating attacks, designing hacking tools, and drafting network-infiltration strategies.” China vehemently denies any connection between hackers and the PRC. China‘s State Council Information Office said that accusations the hackers are targeting overseas entities are, —groundless, irresponsible and also have ulterior motives.”[13] Much of the information in the *Time* article came from two iDefense reports. iDefense is an Internet security company purchased by VeriSign in 2005. The iDefense report says that the Network Crack Program Hacker receives $271 a month from an unknown benefactor to subsidize its activities.[14]

Network Crack Program Hacker is not the only hacker group in China. Honker Union, Red Hacker Alliance, Titan Rain, GhostNet, and Student Hacker Union are other prominent groups with membership ranging in size from several members to tens of thousands.[15] Tim Stevens with Jane‘s Intelligence Review, reports that the presence of —thousands” hacker groups, —pursuing nationalistic goals,” makes it difficult to determine, ―the lines between civilian and military computer network operations.”[16] Regarding the Red Hacker Alliance, The Heritage Foundation senior analyst James Carafano goes further saying they are, —a Beijing-sanctioned ‗network security‘ organization.”[17] Stevens‘ article states that the most famous of these groups is Honker

Union. Scott Henderson, of the Foreign Military Studies Office reports that Honker Union disbanded in late December 2004 but Chinese newspapers hailed the rebirth of the group only one month later."[18]

It is likely that hacker groups continually reinvent themselves as they, —funded, grow, evolve, and then shift to new names or groupings given their ostensibly illegal nature."[19] Chinese law prohibits hacking and the government has periodically taken legal action against such groups, presumably in an attempt to —demonstrate Beijing's resolution to prevent such activities."[20] Larry Wortzel, in testimony before the House of Representatives Committee on Foreign Affairs, suggests that hacking activity —may be a group of patriotic hackers in China who just hate criticism of the Communist Party."[21]

China continues to develop and improve their capability in conducting computer network operations. The Office of the Secretary of Defense outlined in its 2010 report to Congress on the security developments involving the PRC that, —The RC utilizes a large, well-organized network of enterprises, defense factories and affiliated research institutes and computer network operations to facilitate the collection of sensitive information and export-controlled technology."[22] In a discussion of China's modernization program, the report continues that, —foreign investments, commercial join ventures, academic exchanges, repatriated PRC students and researchers, and state-sponsored industrial/technical espionage," are identified means used to improve, —military research, development, and acquisition."[23] James Clapper, Director of National Intelligence told the Senate Armed Services Committee, —The Chinese have made a substantial investment in [cyber warfare], they have a very large organization devoted to it and they're getting pretty aggressive."[24]

Official Policy

The recent publication of China‘s National Defense White Paper offers the best look into current Chinese policy. Primarily, China states that their defense policy is defensive in nature in accordance with the Constitution of the People‘s Republic of China. This policy has the three principle aims of deterring aggression, defending the nation, and securing social stability. The policy is in line with China‘s political, social, economic, and cultural traditions.[25] Additionally, China subscribes to the policy known as the Five Principles of Peaceful Coexistence. These principles, originally proposed by Chinese Premier Zhou Enlai in 1954, lay the groundwork for preventing conflict between nations. The five principles are mutual respect for territorial boundaries and sovereignty, mutual non-aggression, mutual non-interference in internal affairs, mutual benefit and equality, and peaceful coexistence.[26]

During the period from 1989 to 1991, three significant events changed party officials and military commanders‘ strategic approach to warfare. The student uprising in Tiananmen Square in 1989, the fall of the Soviet Union later the same year, and the 1991 Gulf War heralded in an era to develop a new national strategy. A PLA review of the U.S. performance in the Gulf War showed the strengths in capabilities and weak points for possible exploitation. In particular, the PLA began preparations to integrate information management technology into a strategy emphasizing information warfare.[27] Codified in the 2010 National Defense White Paper, the doctrine of fighting ―local war under informationized conditions," is a requirement in all PLA training and exercises.[28] The white paper further states that ―informationization as the driving force" in their modernization program.[29] China continues to advance its knowledge of joint operational theory, developing new combat forces, and conducting military training all under informationization conditions.[30]

Dean Cheng, a China expert at The Heritage Foundation provides further clarification of ―local wars under high-tech conditions" and ―local wars under informationalized conditions" in testimony provided to the U.S.-China Economic and Security Review Commission in January 2011. Cheng says that there are three assumptions in China‘s strategy: wars are of short duration, will not occupy China but will attack political, economic, and military centers, and will involve all five domains of warfare to control information.[31] Cheng also discusses the idea of the ―three warfares" published in the Chinese People‘s Liberation Army Political Work Regulations in 2003. The three warfares include psychological warfare, public opinion warfare, and legal warfare. Cheng postulates there are three purposes for the ―three warfares." The first purpose is to cause doubt and reduce will to intervene or retaliate. The second purpose is to limit support to the U.S. by foreign governments in restricting or denying access to ports and supply facilities. The third purpose is to reinforce Chinese will needed to sustain a conflict.[32]

As described by Cheng, psychological warfare has the most influence at the strategic level of war and is designed to influence not only military and political leaders but an adversary‘s population as well as China‘s own population. Public opinion warfare attempts to persuade perception and opinion with all types of media. Legal warfare uses interpretations of domestic and international law to achieve favorable conditions for China while simultaneously incapacitating an adversary. The ―three warfares" combine to establish a ―defense in depth that is executed temporally and politically rather than physically.‖[33]

China retains strict control on the use of the Internet. China has 14 different government agencies that share regulatory and enforcement responsibility. As of 2003, there were more than 60 regulations or laws concerning the use of the Internet.[34] ―Many of these laws and regulations are vague and include ―catch-all‖ provisions.‖[35] To this end, China distributed a white paper in 2010 outlining the official policy on the Internet. The paper states, ―The Chinese government has from the outset abided by law-based administration of the Internet, and endeavored to create a healthy and harmonious Internet environment, and build an Internet that is more reliable, useful, and conducive to economic and social development.‖[36] Additionally, the head of China‗s State Council Information Office, Mr. Wang Chen, gave a speech in April 2010 about the Internet to the Standing Committee of the National People‗s Congress. In that speech, Wang outlined five points on the advantages and disadvantages of the Internet.

The first of these five points highlights the use of the Internet to further the formation of ideology and public opinion. Second, is improving the working relationship between government entities controlling the Internet and the need to create laws capable of maintaining government control. Third, is the use of real name identification using personally identifiable information to access the Internet and eliminate anonymity. Fourth, the use of the Internet to post video and other multimedia is a security concern but at the same time improves economic development. Lastly, Wang describes limiting the access of Internet users to ―harmful information.‖[37]

Recent Activities

Reports of cyber attack on websites or the hijacking of email is nothing new. These types of activities along with computer viruses and other forms of malicious software have existed nearly since the first computer network was established. These events generally cause some form of noticeable malfunction to the user, though not in all cases. The use of back door software or robot networks, called botnets, is preferred in cases where the perpetrator does not want the user to recognize system compromise. In either case, these activities leave a digital fingerprint behind that provides a forensic investigator clues to the origin of the attack and help develop a hacker profile.

In 2006, several congressional representatives and committees had their computers compromised by hackers. Representative Frank Wolf (R-VA) and Representative Mark Kirk (R-IL) were two of the targets for the attack. Neither Representative Wolf nor Representative Kirk had information of any criminal value. Representative Wolf had ties to human rights groups and advocates for democracy. Representative Kirk was the co-chair of the U.S.-China Working group. Investigators found that malware designed to establish connections to servers located in China infected each of their computers.[38]

In February 2011, *Reuters* news service reported on a cyber attack against two of Canada‘s economic ministries. Stockwell Day, the Minister of the Treasury Board characterized the attack as, ―not themost aggressive but it was a significant one."[39] The other ministry affected was the Finance Department. The hackers used servers located in China. Speculation by David Skillicorn, a professor at Queen‘s University in Kingston, Ontario suggests that the hackers may be after data regarding Canada‘s commodity industry.[40]

In March 2001, the European Union Parliament network experienced two separate attacks. The email system started experiencing problems on 9 March when system messages started appearing in Chinese. An unidentified European Union official said the attacks —appeared to be coordinated, well organized, and geared towards extracting sensitive information."[41] Initial reports suggested that the timing of the attacks with the European Union Council summit meeting was no accident but an unidentified source at the European Union said, —Suggestions that this attack is somehow related [is] bizarre to say the least." The source went further saying that the attacks were definitely outside the boundary of normal attacks that —this is a major incident."[42]

On April 8, 2010, government and military email traffic passed through China Telecom, a state-owned Chinese telecommunications firm. For a period of 18 minutes, the Internet traffic from the Department of Defense, each branch of service, the National Aeronautics and Space Administration, and the National Oceanic and Atmospheric Administration traveled through China before arriving at its final destination.[43] Reporting in this incident, Fox News interviewed Chris Smoak, a researcher from the Georgia Tech Research Institute, Smoak stated that incidents such as the one that occurred on April 8th happen —two to three times a year."[44] Smoak continues in saying that the routing of Internet traffic was not, —designed with security in mind," and, —that anyone could do this at any time."[45]

The U.S.-China Economic and Security Review Commission 2010 report to Congress describes the process by which servers work in cooperation routing Internet traffic. Internet servers continually monitor the flow of digital data and expedite traffic by the fastest route available. There are 13 main servers located around the world that constantly communicate the details on the amount of Internet traffic and determine which server provides the fastest response. In the case of China Telecom, the server distributed a false signal to the other main servers communicating that it was immediately available causing the information to pass through that location. Subsequently, the other 12 servers around the world started passing information through China. The total amount of information passed through China equaled 15 percent of all Internet traffic.[46]

Beginning in 2003, a group of computer hackers codenamed _Titan Rain‘ by the Federal Bureau of Investigations, extracted 10 to 20 terrabytes of government information over a period of four years. These attacks originated from southern China in the Guangdong province, home to many of China‘s information technology companies. During this time, information from the Defense Information Systems Agency, the U.S. Army Aviation and Missile Command, and the U.S. Army Space and Strategic Defense installation was secretly copied and exfiltrated and sent to servers in Hong Kong and Taiwan before arriving at its final destination in China.[47] In April 2009, several terabytes of information on the F-35 Joint Strike Fighter project were exfiltrated to a computer address in China over the preceding two-year period. The data contained information regarding the fighter‘s capabilities and design. A forensic comparison of the hacking techniques used by _Titan Rain‘ and the perpetrators of the Joint Strike Fighter attack matched one another.[48]

Few companies or governments will publicly acknowledge a breach in their network security measures. This was not the case with Google, an Internet search engine company. In January 2010, Google announced that they had discovered a sophisticated and targeted attack of their corporate infrastructure originating from China, resulting in the loss of intellectual property, most notably the source code for their powerful Internet search engine. In addition to stealing the source code, hackers accessed the Google email accounts of Chinese human rights activists. Google was not the only company targeted in the attack. Investigators discovered 33 other companies conducting business in finance, chemicals, technology, and media were involved. The hackers called themselves ―Operation Aurora."[49]

Operation Aurora conducted reconnaissance of the targeted networks, collecting information on the systems, their structures, and users. Armed with this data, Operation Aurora then exploited several system users using data collected from social networking sites and posing as acquaintances established chat sessions with the victims. During the chat sessions, Operation Aurora hackers would send a benign looking hyperlink to a photo-sharing website for the victim to open. On opening the hyperlink, malware would automatically download on to the users system and provide username, password, and credentials to the hacker. With this information, the hackers would then access the network and exfiltrate the source code information.[50]

Operation Aurora used malware written in Chinese. Just before Google made the announcement of the attack, the only discussion on the Internet was strictly on Chinese language websites. Investigators discovered that the servers used to commit the attack are located in China with the exception of the photo-sharing site and the servers used to conduct the network reconnaissance. Internet security firm iDefense stated, ―a single foreign entity consisting either of agents of the Chinese state or proxies thereof," committed the attack.[51]

There is little evidence that directly links the attacks to the Chinese Communist Party of the government of China. Current forensic techniques are insufficient to determine much more than the location where the attacks originated. There are however consistencies between these attacks that are agreed upon by the authors on this subject. All of the attacks originated from mainland China using very sophisticated hacking techniques. The software is unavailable to the public and written exclusively in Chinese. Each of the attacks had extensive intelligence gathering before the exfiltration of the data and the data captured had little criminal value but more political value.

History, Culture, Politics, and Religion

The history of China dates back for thousands of years but it is the convergence between east and west in the mid-nineteenth century that is most important. The First and Second Opium Wars from 1839-1842 and 1856-1860 saw the loss of China sovereignty to the British. By 1830, British traders in Canton traded opium for Chinese goods and tea. Opium dens sprang up all over China and drug addiction was a serious problem facing the Qing Dynasty. The year 1836 saw the first official response to the opium trade as the government outlawed opium then began systematically to close the opium dens. Chinese officials also confiscated opium from the traders resulting in armed conflict between the parties. China claimed that all foreigners and the foreign controlled economic exclusion zones must abide by Chinese law. Britain claimed that the exclusion zones were under British rule and only British laws applied within the zone.[52]

By the end of the war, Britain retained complete control over the exclusion zone and exacted a penalty from the Chinese enacting decidedly lop-sided trade agreements. The year 1856 saw a repeat of the same conflict on the right of sovereignty when Chinese soldiers boarded a British ship in Canton harbor and detained the crew. Known as the 2nd Opium War or the Arrow War, this renewed hostilities between Britain and China. Ultimately, the result was the same and a defeated China found itself offering further concessions and renewed trade agreements strengthening Britain‘s position. Colonial powers began to divide China and operated more and more trade zones.[53]

Richard Hooker, a professor at Washington State University writes about the impact the Opium Wars has on present day China. To this day China considers the outcome of the Opium Wars to be their most humiliating experience and view it as the low point in China‘s history.[54] For thousands of years the Chinese considered themselves as the most advanced culture and the rightful hegemon of the world. This Sino-centric view developed from Chinas interaction with its less cultured and advanced foreign neighbors. Known as the Middle Kingdom, China considered itself the center of the known world surrounded by barbarians.[55] For many years, this perception was true but the Age of Industrialization in Europe quickly catapulted European capabilities far beyond that of the Chinese. The Europeans forced China to accept defeat and humiliation causing a deep seeded contempt toward them and those who offered the Europeans assistance or at least did not intervene on the behalf of the Chinese.[56] This latter group included the Americans. Such a dislike, and perhaps even hatred, for foreigners existed that with support from the Qing dynasty, some Chinese took up arms in 1900 in the Boxer Rebellion in an attempt to drive the invaders from China.[57]

Unlike many western cultures, Chinese culture is fundamentally philosophical in nature rather than based on material goods or wealth. Concepts such as time, power, and wealth are radically different from western ideas of the same concepts.[58] A Chinese concept of time lacks the urgency or need for immediate action seen in western cultures. As with other cultures, China has its own stories, fables, axioms, and sayings passed down from generation to generation that are an integral part of Chinese culture. The 36 stratagems is one example of these sayings compiled over time from many different sources but easily identifiable and recognizable to the Chinese who grew up hearing them from their parents or grandparents. The stratagems are generic enough to allow application in a variety of situations but provide enough information to communicate the concept or idea.[59] Similar to the stratagems are the writings of Sun Tzu and other military strategists. Chinese proverbs provide another set of maxims that inculcate culture from generation to generation. As stated by Gao Yuan, ―taken singly, they provide explanations of phenomena . . . taken as a whole, teach a way of thinking."[60]

Politically, emperors ruled China for centuries until 1911 when the last Qing dynasty emperor was overthrown. A period of relative turmoil ensued characterized by fighting between competing warlords, the struggle of the Nationalist party to establish power, the Japanese invasion into Manchuria, and the rise of the communists led by Mao Zedong. In the end, Mao and the Chinese Communist Party were the victors and established a tight control over the governance of China. The main goal of the Chinese Communist Party is to remain in power and to restore China to its former position as the rightful hegemon.[61]

The idea of a single seat of government power with ultimate authority dates back 3000 years. Established around 1000 BCE, the mandate of heaven states that the right to govern comes directly from heaven. The mandate also states that the right to rule applies to one ruler at a time. Further, the right to rule will continue based on the performance of the ruler acting as a steward of heaven. Poverty, famine, and natural disasters are signs that the ruler no longer has the mandate of heaven. The mandate provides legitimacy to a strong central ruler or government while simultaneously subordinating other claims to rule unless an event such as famine occurs.[62]

China has no official state religion but many Chinese follow the teachings of Confucius. Based on a hierarchy of standing in personal relationships, Confucianism is a way to maintain social harmony and order. Known as filial piety, people tend to associate the hierarchy with a young person showing respect and deference to an elder. Confucius based his philosophy on the concept of filial piety and extended it to characterize five relationships between the junior and the senior based on social standing. The five bonds are ruler to subject, father to son, husband to wife, brother to brother, and friend to friend. While Confucianism is not a religion in a strict sense, it does offer a way to live one‘s life and establishes social order in society. Much of Chinese culture follows the basic principles of Confucianism to this day.[63]

Internal and External Threats

Viewed from the Chinese perspective, there are several threats that China currently faces. Internally, the Chinese Communist Party views the provinces of Tibet and Xinxiang as two sources of internal instability. Tibet was autonomous from China for 950 years before the Chinese Communist Party assumed power in 1949. Xinjiang, which is mostly Muslim, came back under the umbrella of Party rule after Joseph Stalin agreed to turn over the area to Mao in 1950. Russia had acquired Xinjiang during the time of Russian Imperialism. Dissatisfaction among the people of Tibet and Xinjiang led to a series of uprisings that the government quickly repressed, though Tibet continues to fight for independence.

Taiwan remains a sore spot in the PRCs history. Relations between Taiwan and mainland China have improved over the years but China clearly states that the ultimate goal is the reunification of Taiwan under the control of the PRC. Taiwan asserts the same goal of reunification but under the auspices of the Republic of China. This is the point of divergence between the two. In 1996, China conducted a series of military exercises off the coast of Taiwan during the first-ever Taiwanese elections. These exercises were a deliberate show of force to both the U.S. and Taiwan, suggesting that China would use military force if necessary to prevent Taiwan‘s independence. Recently, China and Taiwan have normalized trade, travel, and mail between them.

Human rights activists, pro-democracy groups, and other dissidents constitute a threat to the authority of the Chinese Communist Party and social stability. People such as artist Ai Weiwei who are critical of the government find themselves quietly removed from society. The student demonstrations in Tiananmen Square in 1989 saw the PLA use tanks and deadly force to clear the students from the area. The result was the death of hundreds of protestors.

Aside from the internal human threat, China faces a host of other problems ranging from environmental concerns, poor infrastructure, energy, lagging technology, low world opinion, low wages, a rising middle class, and an aging population. Particular to the issue of cyber warfare is the discrepancy between China‘s level of technological expertise and that of the United States. China understands that in order to compete on the world economic stage, they must have access to technology. Unfortunately, it takes years to develop the capabilities to innovate, produce, distribute, and implement technology. Instead, China opts for a different approach of reverse engineering products or simply acquiring the technical data from other sources.[64]

Regarding external threats, China considers the U.S. as the preeminent external threat. In 1994, the Chief of the General Staff said in a speech that the —American hegemonists” were —opposing and subverting” the Chinese Communist Party and the youth of China.[65] China‘s leaders feared that the ending of the Soviet Union and the strength of the U.S. military as demonstrated in the 1991 Gulf War caused U.S. leaders to focus their efforts in restraining China.[66] China views the recent spread of democracy in South Korea, Japan, and India and the alignment of these countries with the U.S., as a means of hedging China‘s increasing military strength, as American intervention to contain China.[67] The uprising in Tiananmen Square and the subsequent U.S. sanctioned economic constraints, the fall of the Soviet Union, and the invasion of Panama combined with the 1991 Gulf War all lead China to the conclusion that the, —United States [is] the main enemy at present and into the future.”[68]

Summary

China has the capability to conduct cyber warfare directly with IW militia units as well as the Technical Reconnaissance Bureaus and indirectly through hacker organizations. China‘s official policies promote security from a purely defensive posture, seek to promote peace through cooperation, and provide freedom speech and access to the Internet. Recent activities suggest that computer network attacks are originating in China but forensic investigators are unable to link the attacks to the China, the Chinese Communist Party, or the PLA. History and culture influence the Chinese way of thinking. Lastly, China faces both internal and external threats and these threats affect their overall strategy.

[1] Krekel, 30.

[2] Carolyn Bartholomew, Chairman, *2009 Report to Congress of the U.S.-China Economic and Security Review Commission* (Washington, DC: Government Printing Office, November 2009), 172.

[3] Krekel, 33.

[4] Ibid., 35.

[5] Ibid.

[6] Ibid., 32.

[7] Ibid., 36.

[8] Bartholomew, 174.

[9] Krekel, 35.

[10] Ibid., 32.

[11] Ibid.

[12] Ibid.

[13] Simon Elegant, ―Enemies at the Firewall," *Time* (6 December 2007), http://www.time.com/time/magazine/article/0,9171,1692063-1,00.html (accessed 26 April 2011).

[14] Ibid.

[15] Scott Henderson, *The Dark Visitor: Inside the World of Chinese Hackers* (Fort Leavenworth, KS: Government Printing Office, January 2007), 1-145.

[16] Tim Stevens, —Breaching Protocol – the Threat of Cyberespionage," *Jane's Intelligence Review* (11 February 2010).

[17] James Carafano, —Obama Needs to Address Our Cyber-Warfare Gap with China," *The Heritage Foundation*, 23 January 2011, http://www.heritage.org/Research/Commentary/2011/01/Obama-Needs-to-Address-Our-Cyber-Warfare-Gap-with-China (accessed 27 April 2011).

[18] Henderson, 55-58.

[19] Stevens, *Jane's Intelligence Review*.

[20] Ibid.

[21] Larry Wortzel, —China‘s Approach to Cyber Operations: Implications for the United States," Testimony before the Committee on Foreign Affairs in the Hearing on"The Google Predicament: Transforming U.S. Cyberspace Policy to Advance Democracy, Security, and Trade (Washington, DC: 10 March 2010), 3.

[22] Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China* (Washington, DC: Government Printing Office, 2010), 6.

[23] Ibid., 41.

[24] Reuters, —China‘s Cyber Abilities Worry U.S. Spy Chief," 10 March, 2011, http://www.reuters.com/article/2011/03/10/us-china-usa-cyber-idUSTRE7295Y820110310 (accessed 12 March 2011).

[25] Information Office of the State Council, —China‘s National Defense in 2010" (Beijing, China: Xinhua News Agency, March 2011), http://www.chinadaily.com.cn/china/2011-03/31/content_12256413.htm (accessed 3 April 2011), 2.

[26] Consulate General of the People‘s Republic of China, http://houston.china-consulate.org/eng/nv/t140964.htm (accessed 3 March 2011).

[27] June Teufel Dreyer, —Recent Developments in the Chinese Military," in *A Military History of China*, ed David A. Graff and Robin Higham (Boulder, CO: 2002), 285-288.

[28] Krekel, 6.

[29] OSC, —China‘s Naitonal Defence in 2010."

[30] Ibid.

[31] Dean Cheng, —China‘s Active Defense Strategy and its Regional Impact,” *The Heritage Foundation,* 1 February 2011, http://www.heritage.org/ Research/Testimony/ 2011/01/Chinas-Active-Defense-Strategy-and-Its-Regional-Impact (accessed 26 April 2011).

[32] Ibid.

[33] Ibid.

[34] Slane, 228-229.

[35] Ibid., 244.

[36] Information Office of the State Council, —The Internet in China” (Beijing, China: Information Office of the State Council, June 2010), http://www.china.org.cn/ government/whitepaper/2010-06/08/content_20208007.htm (accessed 20 April 2011).

[37] Slane, 226-228.

[38] Bartholomew, 180.

[39] David Ljunggren, —Canada Says Cyber-attack Serious, Won‘t Harm Budget,” *Reuters* (Ottawa, Canada: 17 February 2011), http://www.reuters.com/article/ 2011/02/17/us-cyberattack-idUSTRE71G0RG20110217 (accessed 3 April 2011).

[40] Ibid.

[41] John Leydon, —EU Parliament Suspends Webmail after Cyber-attack,” *The Register* (London, United Kingdom: 31 March 2011), http://www.theregister.co.uk/2011 /03/31/eu_parliament_hack (accessed 3 April 2011).

[42] Ibid.

[43] Slane, 244.

[44] Joshua Rhett Miller, —Internet Traffic from U.S. Government Websites was Redirected Via Chinese Networks,” *Fox News*, 16 November 2010, http://www.fox news.com/politics/2010/11/16/internet-traffic-reportedly-routed-chinese-servers/ (accessed 5 March 2011).

[45] Ibid.

[46] Slane, 244.

[47] Stevens, *Jane's Intelligence Review.*

[48] Ibid.

[49] Slane, 238-239.

[50] Ibid.

[51] Slane, 239.

[52] Richard Hooker, —Ch'ing China: The Opium Wars," Washington State University (1996), http://www.wsu.edu:8080/ ~dee/CHING/OPIUM.HTM (accessed 20 April 2011).

[53] Ibid.

[54] Ibid.

[55] Richard Hooker, —Ancient China: The Chou," Washington State University (1996), http://www.wsu.edu:8080/~dee/ANCCHINA/ANCCHINA.HTM (accessed 20 April 2011).

[56] Hooker, —Ch'ing China: The Opium Wars."

[57] Richard Hooker, —Ch'ing China: The Boxer Rebellion," Washington State University (1996), http://www.wsu.edu:8080/~dee/CHING/BOXER.HTM (accessed 20 April 2011).

[58] Dean Cheng, Moderator, —China and Cyber Security," *The Heritage Foundation* (April 2010), http://www.heritage.org/Events/2010/04/China-and-Cybersecurity (accessed 26 April 2011).

[59] Gao Yuan, —Lure the Tiger Out of the Mountains: The 36 Stratagems of Ancient China" (New York, NY: Simon and Schuster, 1991), 16.

[60] Ibid.

[61] William Maxcy, —China: Mitary Art, Wars, and Revolution" (lecture, Command and General Staff College, Fort Leavenworth, KS, March 2011).

[62] Hooker, —Ancient China: The Chou."

[63] Maxcy, —China: Military Art, Wars, and Revolution."

[64] Jason Fritz, —How China will use cyber warfare to leapfrog in military competitiveness," *Culture Mandala: The Bulletin of the Centre for East-West Culture and Economic Studies* 8, no. 1 Article 2 (1 October 2008): 33-39, http://epublications.bond.edu.au/cm/vol8/iss1/2 (accessed 11 May 2011).

[65] Constantine Menges, —China: The Gathering Threat" (Nashville, TN: 2005), 120-123.

[66] Ibid.

[67] John Lee, ―China‘s American Obsession: Why Osama bin Laden‘s Death is Making Chinese Leaders Nervous,” *Foreign Policy*, http://www.foreignpolicy.com/ articles/2011/05/06/china_s_america_obsession?page=0,0 (accessed 9 May 2011).

[68] Menges, 121.

CHAPTER 3

RESEARCH METHODOLOGY

> Leaders are often late to recognize such changes, and even when they do, inertia tends to limit their ability to adapt quickly. Driven by an inherent desire to bring order to a disorderly, chaotic universe, human beings tend to frame their thoughts about the future in terms of continuities and extrapolations from the present and occasionally the past.
>
> — Joint Operating Environment, 2010

The nature of this study requires the use of qualitative design research methods over quantitative. Data from the literature focuses more on China's strategic concepts of information warfare, military doctrine and theory, stratagems, and culture. The discussion on these subjects is mostly metaphysical in nature and has little quantifiable data. The use of information readily available in the public domain lacks quantifiable data due to the sensitive and secretive nature of cyber warfare. Even quantifiable data such as the number of cyber attacks offers little insight since attribution of these attacks is extremely difficult. While a quantitative study would produce accuracy and precision, the data available does not lend itself to such conclusions. For these reasons, the author chose a qualitative approach.

This study takes a holistic approach in understanding the multiple components that influence strategy development. As stated by Harry Yarger in his *Little Book on Big Strategy*, strategy development proceeds from a desire to achieve national objectives using the instruments of national power influenced by adversaries, culture, politics, organization, and resources. Yarger continues by postulating 15 premises of strategy as a means to understanding strategic logic. This study uses five of these strategic premises. The Office of the Secretary of Defense used a similar methodology in the 2010 Annual

Report to Congress stating, ―It is possible, however, to make some generalizations about China‗s strategy based on tradition, historical pattern, official statements and papers, and emphasis on certain military capabilities and diplomatic initiative."[1]

Yarger‗s first premise is that politics is an inherent part of strategy and that achieving political objectives through policy ensures that strategy ―pursues appropriate aims."[2] The second premise is that a strategy is subordinate to the strategic environment. The third premise is that strategy is a human activity and is subject to emotion and affection. The fourth premise is that in pursuing a strategy, the actors will do so to the best of their ability. The final premise is that strategy is dependent on time. It is not readily apparent that these five premises relate to the ideas of capability, policy, activity, culture, and threat presented in chapter two, but a detailed explanation of the strategic premises reveals how they are related.

To begin with, if politics is inherent in strategy then it is crucial to understand the politics of China. This is a relatively easy task as China has only one political party whose intent is to keep the party in power. The presentation of Chinese politics itself is too broad of a topic to discuss in detail therefore this study will focus on the ability of the government to maintain power and control over the Chinese people. Power and control are then two criteria to use in the analysis of politics as part of the discussion on culture, history, politics, and religion. Secondly, the premise also states that policy is the way to achieve political ends. Since policy is a direct result of the political objective, this too becomes a criterion for analysis.

A strategy that is subordinate to the strategic environment has little meaning without explanation of what the strategic environment consists of. The nature of the environment is both physical and metaphysical.[3] The physical nature recognizes the influence on strategy by domestic and external components such as internal and external actors, domestic institutions, and geography. China‘s internal threats, both physical and metaphysical, are the provinces of Tibet and Xinjian, Taiwan, and social unrest. External threats are the U.S., India, Russia, Japan, and South Korea. Criteria for analysis then are internal and external threats. A delimitation of this study is the U.S. as the only external threat.

Strategy is a concept unique to humans alone and as a result, emotion, beliefs, and values influence strategy. The third premise states that strategic design relies on subjectivity as much as objectivity. This subjectivity comes from the metaphysical nature of the strategic environment and deals with values, beliefs, perception, moral judgment, and other philosophical ideas of being or knowing.[4] While less tangible than the physical components, these ideas influence the way people think about or approach strategy. These engrained characteristics make it difficult to know when they influence thought and inject bias into the process. This premise as a criterion is culture.

The fourth premise states nations will pursue their national interests to the best of their ability.[5] By design, strategy confers advantage to a nation by creating favorable conditions using national power to achieve national interests. Strategy is key in the, ―pursuit, protection, or advancement of these interests."[6] The instruments of national power are military, economic, diplomatic, and information. In the case of cyber warfare, this study looks at the use of the military instrument of power as a means to achieve the national interest. Specifically, this is a review of China‘s military capabilities to conduct cyber warfare. Criteria for analysis are specialized military units, hackers, and technology.

The final premise is that strategy is dependent on past events as well as future events. The common factor linking past and future events is time. Strategy without the consideration of the outcome of past events is, ―lessikely to be successful," lacks continuity with the present and perspective toward the future.[7] This implies that analyzing past events with the knowledge of the ultimate goal, will lead to a strategy by deduction. Therefore, analyzing China‘s recent cyber events and activities provides a narrow range of possible strategies and is a criterion for analysis. A design approach using these criteria: specialized military units, hackers, technology, policy, cyber activities, power, control, culture, internal, and external threats, is a holistic approach capable of developing an understanding of China‘s cyber strategy.

[1] OSD, ―Military and Security Developments Involving the People‘s Republic of China," 13.

[2] Harry R. Yarger, ―Strategic Theory for the 21st Century: The Little Book on Big Strategy," 38; CGSC C200 Book of Readings (Fort Leavenworth, KS: Government Printing Office, 2010), 38-43.

[3] Ibid.

[4] Ibid.

[5] Ibid.

[6] Ibid.

[7] Ibid.

CHAPTER 4

ANALYSIS

Background

In chapter 1, this study presented several questions asking what cyber warfare strategy is China pursuing and does it mean to have ―Chinese characteristics?” It is impossible to determine China‘s cyber warfare strategy with absolute certainty, as open source documents do not provide all of the information to make such a determination. However, by piecing together the available information, showing the linkage between them, and analyzing the data, it is possible to develop a likely strategy that closely approximates reality. In order to understand this strategy and specifically one with ―Chinese characteristics” this study focuses on answering questions as individual entities then ties them together through analysis.

Strategies develop out of necessity and have a distinct or underlying purpose. The driving force behind a nation developing a strategy could be a response to a significant change in the geo-political environment. An example is the ending of the Cold War that required the U.S. to develop a new strategy postured to address a new set of concerns. In China‘s case, Deng Xiaopeng‘s economic reforms in the 1982, and their revitalization in again in the early 1990s along with the four modernization programs of improving: industry, science, technology, and agriculture, began the internal shift of China‘s strategic vision. These four modernization programs were an attempt to reform China following the, ―great catastrophe,” of Mao Zedong‘s Cultural Revolution.[1] This shift continued to evolve in response to other events such as the student led uprising in Tiananmen Square in 1989 and the fall of the Soviet Union later that same year. Another major event influencing China‘s strategic approach was the U.S. led 1991 Gulf War. These events changed China‘s strategic environment and precipitated an awakening of Chinese leaders to the new realities and the requirement for new strategies.[2]

This new environment posed some significant challenges to the PRC. First, was the growth of the economy as a means to achieve parity among the world‘s leading nations. In 1992, China‘s gross domestic product was 422 billion (USD). By 2002 the economy tripled to 1.4 trillion (USD) and in 2009 the economy tripled again to 4.98 trillion (USD).[3] The rapid expansion of the economy provided the monetary means to modernize and sustain improvements in industry, science, and technology as outlined by Deng, but this expansion came at a price in the form of inflation and urban migration. Concerned by these negative impacts of reform, party leaders slowed the reformation process resulting in student led demonstrations calling for the reforms to continue and at a much faster rate.[4]

Second was the student uprisings in response to the governments halt of socio-economic reform. What started as a student gathering over the death of Hu Yaobang, a popular political figure and former Party General Secretary, turned into a political demonstration that quickly spread beyond Beijing.[5] The People‘s Daily, a CCP news outlet described the massive gatherings as, —a planned conspiracy and a disturbance. Its essence is to, once and for all, negate the leadership of the CCP and the socialist system,” and called for the disturbance to be —checked resolutely.”[6]

Students, intellectuals, businesspeople, factory workers, and even members of the military who felt disenfranchised by the government participated in the demonstrations. The demonstrations spread around the country to other cities as well. Demonstrations in

Guangzhou, Chengdu, and Shanghai began calling for an end to corruption, democratic reforms, and personal freedoms.[7] Government attempts to disperse the crowds and regain control over the civil disobedience failed and the PLA was ordered to remove the demonstrators from Tiananmen Square in Beijing.

In less than 24 hours, the PLA cleared the square and hundreds if not thousands of demonstrators were dead.[8] The Chinese government immediately tried to cover up the incident by forbidding hospitals to release any information on those killed or wounded and stating publicly that there were no casualties. Two weeks later in an interview with *NBC News*, an unidentified Chinese government spokesperson emphatically stated that, ―No one was shotdown or crushed under the wheels of vehicles. The reports that there was a blood-bath and that many people were crushed were incorrect."[9] The actions of the Chinese government and particularly the hardliners in the Chinese Communist Party, made it clear that they would result to all means available in order to maintain political control and their idea of social stability.[10] International reaction criticized China‘s handling of the affair and the U.S. ceased military sales and ended nuclear cooperation. This only incensed the Chinese government who accused the U.S. of meddling in China‘s internal affairs.[11]

Third, in November 1989, the Soviet Union began losing its control over Eastern Europe. The fall of the Soviet Union to political liberalism served to strengthen China‘s preference for less risky economic reform over political reform.[12] Chinese officials also viewed the demise of communism in Eastern Europe as America‘s attempt to sway people from communism toward democracy. Hardline party members claimed that this trend, known as ―peaceful evolution," was the reason behind the uprising in Tiananmen

Square and they went further to say that, —foreign hostile forces led the movement with the intention of exterminating us."[13] As Eastern European countries democratized, China found itself in the precarious position no longer able to manipulate the U.S. against the Soviet Union to further its own interests. China decided to align with Russia instead of the United States. The Russian Federation was the likely choice particularly since Russia had an abundance of military weapons and was eager to sell them to help boost their failing economy.[14] China realized the need for these weapons once they witnessed the capabilities of American military forces in the 1991 Gulf War resulting in the destruction the Iraqi Army in a matter of days.[15] Additionally, China's leaders feared that the U.S. would focus on a policy of containing China now that the Soviet Union was no longer a threat.[16]

Lastly, it is likely that the Gulf War had the greatest impact on devising a cyber warfare strategy with —Chinese characteristics." After a thorough review of America's success in Kuwait, PLA leaders were —despondent" and realized the need to make significant changes if they ever wished to take their, —proper place in the New World Order."[17] Of all the lessons learned from the Gulf War, the Chinese realized that the effectiveness of the U.S. military relied on technology but more importantly on its ability to manage information with that technology. The use of satellites and other forms of digital C4ISR systems provided a significant advantage over an adversary.[18] China reasoned that such an advantage could be a disadvantage as well and was vulnerable to exploitation.[19] With this realization, the PLA began a transformation of the military with the directive to prepare for, —local wars under high-technology conditions."[20]

Capabilities

Over the past 20 years, China continues to refine their military doctrine reformation and build fighting forces capable of winning —war under conditions of informatization.”[21] To this end, China issues guidance through documents known as Military Strategic Guidelines as a means to control the development and use of military forces. The PLA does not publicly distribute these documents but researchers have determined that the current guidelines date back to 1993, which suggests the influence of the 1991 Gulf War and possibly the collapse of the Soviet Union on China‘s strategic thinking and transformation.[22] One of the key components of the guidelines asserts the need to build forces for —information-age warfare.”[23] Chinese military strategists continue to debate the nature of modern warfare from a historical viewpoint in order to understand concepts such as —revolution in military affairs” and “informatized” war.[24]

One of the PLAs key players in proposing theory and developing IW doctrine is Major General Dai Qingmin. By 1999, Dai began publishing his thoughts and ideas on controlling the electromagnetic spectrum. Dai wrote in his book, *An Introduction to Information Warfare* about the combined use of electronic and network warfare to control the electromagnetic spectrum. Written when he was a faculty member at the PLAs Electronic Engineering Academy, *An Introduction to Information Warfare* was Dai‘s first book on IW.[25] In 2002, Dai published *An Introduction to Integrated Network Electronic Warfare* and an article on the necessity for IW to focus on the protection and destruction of integrated command networks.[26] Each publication received official support from the Chief of the General Staff, General Fu Quanyou.[27] Dai is one of several authors writing about IW and postulating possible strategies. However, Dai‘s works have received the most attention from senior leaders and gained official approval at the highest levels of the PLA. When taken in context with Dai‘s promotion in 2000 to head the 4th GSD, which has responsibility for electronic counter measures and research and development of IW offensive capabilities, it is likely that Dai is the leading subject matter expert and designer of China‘s IW doctrine.

As proposed by Dai, INEW is a means to reduce risk to conventional forces by allowing them to operate without detection by the enemy.[28] This occurs by disabling or suppressing an enemy‘s capability to use C4ISR assets. The intent is to create small windows of opportunity that “blind” an enemy and allow freedom of maneuver.[29] By combining elements of EW such as jamming and deception along with elements of CNA that include disruption of information transfer, virus attacks, or hacking this creates a temporary information blackout.[30] Some advocates of INEW, including Dai, suggest that attacking only critical strategic nodes is required in order to achieve the objective.[31]

If INEW is China‘s IW doctrine, then the implications of such a doctrine requires further analysis. First is the requirement for units or organizations that are capable of conducting the necessary attacks. Second is the need for these units or organizations to have the capability to conduct reconnaissance and identify the critical strategic nodes. Taken further, these units must have the requisite technical skills and access to the most advanced hardware infrastructure and software design support in order to accomplish the mission.

Addressing the issue of the unit/organization requirement first, an analysis of China‘s capabilities shows the initial development of the technical reconnaissance bureaus as early as 1997. Given the timing of the development of the bureaus, after the

1993 Military Strategic Guidelines but before Dai‘s seminal work on IW, it is possible that the bureaus were a proof of concept as a first step towards the informationization of an organization. Currently, China has six TRBs located in the Beijing, Lanzhou, Jinan, Chengdu, and Guangzhou military regions. These bureaus have the responsibility to collect signal intelligence information, which is a function of the 3rd GSD. The 3rd GSD also has responsibility for CND and CNE operations. The association of the TRBs with the 3rd GSD makes the most sense due to the requirement for linguists and technical analysts to properly conduct signals intelligence. It is unknown the exact role of the TRBs regarding CNO but the Security Council Information Office, China‘s official mouthpiece, has published accounts of the bureaus receiving awards for ―research in information warfare theories" and ―achievements in informatization building."[32] TRB staff members conduct information assurance for other PLA units, which suggests the responsibility to conduct network deterrence.[33]As a result, the bureaus most likely report to the 3rd GSD and conduct signals intelligence as well as CND and CNE missions. Additionally, if the TRBs were a proof of concept, conducting network deterrence is the easiest aspect of CNO to begin developing and offers the least amount of risk or exposure to external entities.

The first proof of concept IW militia units appeared in 2002, which coincides with the publication of Dai‘s book on INEW. The units are a conglomeration of information technology professionals and academics considered ―politically reliable" by the State. [34] By targeting a select audience and not filing the unit with new recruits or members of existing units, the PLA ensured that unit members had the requisite skill set and would remain quiet about the operation. The PLA would have known the sensitive nature of the unit‘s mission and the future plans otherwise they would be so selective.

Addressing the need for access to hardware and software, the IW militia units incorporated into information technology firms, thereby providing direct access to the most sophisticated software and best hardware available. This was a logical choice since the unit members came from these institutions and corporations in the first place. Viewed as a model of success, the Academy of Military Science in Beijing outlined a plan in 2003 to continue incorporating militia units with telecommunications firms to make the best possible use of infrastructure, technical experts, and to receive financial support. This strongly suggests that the proof of concept was such a success, the PLA decided to implement the incorporation plan immediately after one year of study.

After publishing this concept, four additional IW militia units known as ―Militia Information Technology Battalions" appeared in the Guangzhou Military Region. Guangzhou is the heart of China‘s telecommunications and information technology industry similar to Silicon Valley in the California. The battalions conducted research on ―launching hacker attacks, propagating viruses, jamming information channels, and disrupting nodes of enemy networks," all of which are forms of Dai‘s INEW attacks.[35] Given that the battalions conducted research on CNA operations, they likely report to the 4th GSD, at the time headed by Dai, and have the primary responsibility of carrying out offensive IW under the INEW doctrine.

In 2006, the Academy published a follow-on article that fully supported the creation of more battalions and suggested the addition of psychological and electronic warfare to the battalion mission. The addition of these missions to the IW battalions would create a single unit capable of conducting EW, CNA, and psychological warfare. This suggestion combines traditional and informationized missions with the ―three warfares" concept. The "three warfares" is the PLAs definitive political doctrine and combines the use of legal, psychological, and the media, as a means to wage war.[36] First published in the Chinese People‘s Liberation Army Political Work Regulations in 2003, the regulation specifically states the conduct of political work is the use of the ―three warfares" of psychological, public opinion, and legal warfare.[37] The Chinese employ psychological warfare as a method to gain strategic, operational, and tactical advantage over an adversary by demoralizing the enemy‘s will to fight while simultaneously bolstering the Chinese people. The use of media to fight the battle of public opinion aims to build domestic support and positively influence international opinion. Public opinion also attempts to abandon policies that are contrary to China‘s national interest. Lastly, legal warfare takes advantage of insufficient, nonexistent, or reinterpretation of international laws. China uses these legal gaps to create domestic law favorable to their national interests. This allows China to claim they are acting in accordance with all laws and regulations.

Placing an emphasis on recruiting people with the proper technical skills, the article stated that relaxed entry standards, such as age or level of physical fitness, be overlooked in order to prevent the disqualification of otherwise highly skilled personnel. The article recommended the need for strict security precautions to prevent the compromising of software tools or information leaks based on the highly sensitive nature of network reconnaissance and the chance such activity could be an act of war.[38] This statement conflicts with the earlier suggestions that CNE is the purview of the 3rd GSD. There are two possible explanations for this.

The INEW doctrine calls for targeting strategic nodes and that requires extensive reconnaissance to determine where the nodes are and what is required to disable them. The first explanation, though unlikely, is that the TRBs conduct CNE, develop a target package, and then hand it off to an IW militia unit for execution. Instead, a second and more plausible explanation is that the TRBs focus solely on defensive capability, which is more in-line with the 3rd GSD mission, and the IW militia units assume all CNA and CNE responsibility. This explanation aligns better particularly since Dai is the author of the INEW doctrine and headed the 4th GSD.

In 2008, the PLA reported that a Lanzhou Military Region militia unit conducting network warfare research had the additional task to, —attackhte enemy‘s wartime networks."[39] Organized into four entities, this same unit focuses on information warfare, information gathering, network warfare, and network protection.[40] While the examples presented focus on the wartime mission for the militia units, speculation is that a peacetime mission includes network reconnaissance to develop plans for computer network attack.[41] This is a modification of the 2006 concept and highlights the evolution of the PLAs thinking. Instead of units focused on a singular specialty like CND or CNE, the most recent IW militia units are task organized with the capability to conduct all aspects of CNO. From a command and control perspective, there is one IW militia unit located in each of the seven military regions in China. By combining CNA, CNE, and CND operations into a single unit, each military region commander would have the capability to conduct CNO with organic assets. Further, these units would consolidate under the 4th GSD instead of divided between the 4th GSD and the 3rd GSD.

Apart from military organizations with cyber capabilities, China has a large number of hacker groups and organizations operating in the country. Groups like Titan Rain, Red Hacker Alliance, and Honker Union conduct malicious network activities from the relatively benign defacing of websites to the much more serious exploitation of sensitive governmental network. Known as honkers, Chinese for red visitor, these hacker groups see themselves as patriotic citizens who are fighting for their country and defending it from foreign attacks.[42] Honkers tend to be, —creative, patriotic, capable, and motivated," and in the context of a people's war, where the population mobilizes on behalf of the nation, honkers become an essential component of comprehensive national power.[43]

The Information Warfare Monitor, a Canadian public-private research venture in tracking cyber espionage, conducted extensive research on the hacker group GhostNet and published a detailed report on their findings. Information Warfare Monitor discovered that GhostNet infected 1,295 computers in 103 countries and that 30 percent of the infected networks are high-value targets including government ministries and embassies.[44] The nature of the attacks, targets, level of sophistication, and the use of servers located in China identify serious network security concerns and the possibility of Chinese government involvement. If the Chinese government is involved, the best explanation of this activity is exploitation for —military and strategic-intelligence purposes."[45]

There is no clear link between the hacker groups and the Chinese government. This then creates a situation where China allows the hacker groups to exist for some national purpose and that the benefits that these groups provide outweigh the inherent risks. First, the Chinese government knows of the existence of the hacker groups. Specifically the PLA sponsors hacker competitions awarding cash, new computer equipment, and in the case of Tan Dailin, a.k.a. Withered Rose, offers training and an annual income. However, if the Chinese government openly supports hacker groups they no longer have the ability to deny support of the hacker group activities. Conversely, by not directly supporting the groups and maintaining control over hacker activities, the government runs the risk of these groups inciting social unrest or worse, conducting activities that incites political backlash from the international community. Therefore, there must be a high level of confidence by Party leaders that these groups will focus their efforts on foreign entities or dissidents within China but not on the CCP.

Confident or not, it is not likely that the CCP would allow the hacker groups free reign with no oversight. This suggests that the Chinese government has plan in the event that hacker activity goes beyond the wishes of the Party. As a fail-safe measure, Chinese officials have the capability to either shut down or block access to the hacker websites. Chinese law requires all websites to register their domain name and in cases where organizations failed to register or pay the domain fees, the websites were shutdown.[46] The Chinese government monitors web activity through the service providers and has the capability to restrict access. Hacker groups are not exempt yet they develop websites, blogs, and share hacking tools and information openly online without government reprisal.

The most logical reason that the government allows this activity is they are receiving valuable information or other benefits from the hackers. In doing so, the hacker groups become a massive de facto intelligence gathering organization. With activities ranging from website defacement to industrial espionage to network reconnaissance possibly hundreds of thousands hackers can provide a great deal of information.[47] This also explains why the PLA would sponsor hacker competitions and provide money, training, equipment to the winners. Chinese officials can identify the best hackers and possibly press them into the service of China by hacking into foreign government computers.[48] In one case, a Chinese police officer attended a hacker convention in a downtown Beijing hotel. When asked why he was at the convention, the officer replied, —We‘re looking to see whether they have anything we can use. If they do, we‘ll contact them.”[49]

Operating clandestinely through a proxy group may be China‘s best approach. It is difficult, if not impossible, to ascertain with absolute certainty that a cyber attack actually occurred in the country where the attack originated. The best that forensic analysts can do is to determine the location of the server used in the attack, but it is possible that control of the server occurs thousands of miles away. This is the attribution problem and creates plausible deniability for the Chinese government. A technique used frequently by Chinese officials is to outright deny any involvement, accuse the accuser, and demand absolute proof of the egregious event. On the few occasions when foreigners have approached Chinese officials with claims of cyber espionage or hacking, China has refused to conduct an investigation.[50] Additionally, PLA sponsored hacking competitions allow them to identify the best hackers and likely the best choice for the most sensitive activities of hacking foreign government networks.

Official Policy

In 1954, former Chinese Premier Zhou Enlai outlined the Five Principles of Peaceful Coexistence. Based on the ideas of respect of a nation‘s sovereignty, non-interference in internal affairs, non-aggression, mutual benefit, and peaceful coexistence, the Five Principles set China‘s policy with India regarding a border dispute over portions of Tibet. Since then, China continues to assert that the Five Principles are the way that China will conduct business with the rest of the world.[51] China‘s 2010 National Defense white paper redefines the Five Principles as —new security concepts” based on —mutual trust, mutual benefit, equality, and coordination.”[52] China maintains that it pursues a, —foreign policy of peace,” and national security that, —is defensive in nature.”[53] Statements like these are an attempt to reassure the international community and particularly the United States.

China sees itself perfectly positioned as a rising national power capable of restoring the glory and prestige of the Middle Kingdom. Economic prosperity is the key to China‘s success. China‘s National Defense white paper states, by connecting their interests, development, and security, to the international community, China will continue to grow.[54] China intends to continue economic expansion that will support modernization programs for their military and create a —moderately affluent” society.[55] This economic growth, peaceful interaction with regional neighbors, and a modernized military are part of the larger campaign to improve international status and regional influence. While mostly economic in nature, regional influence includes a military presence as well. The desired effect of economic and military pressure is to bring Taiwan and disputed territories under the control of the CCP. China will continue to follow this strategy until all historical lands once again reunite under the Middle Kingdom. From a Chinese view, the Middle Kingdom includes more than mainland China.

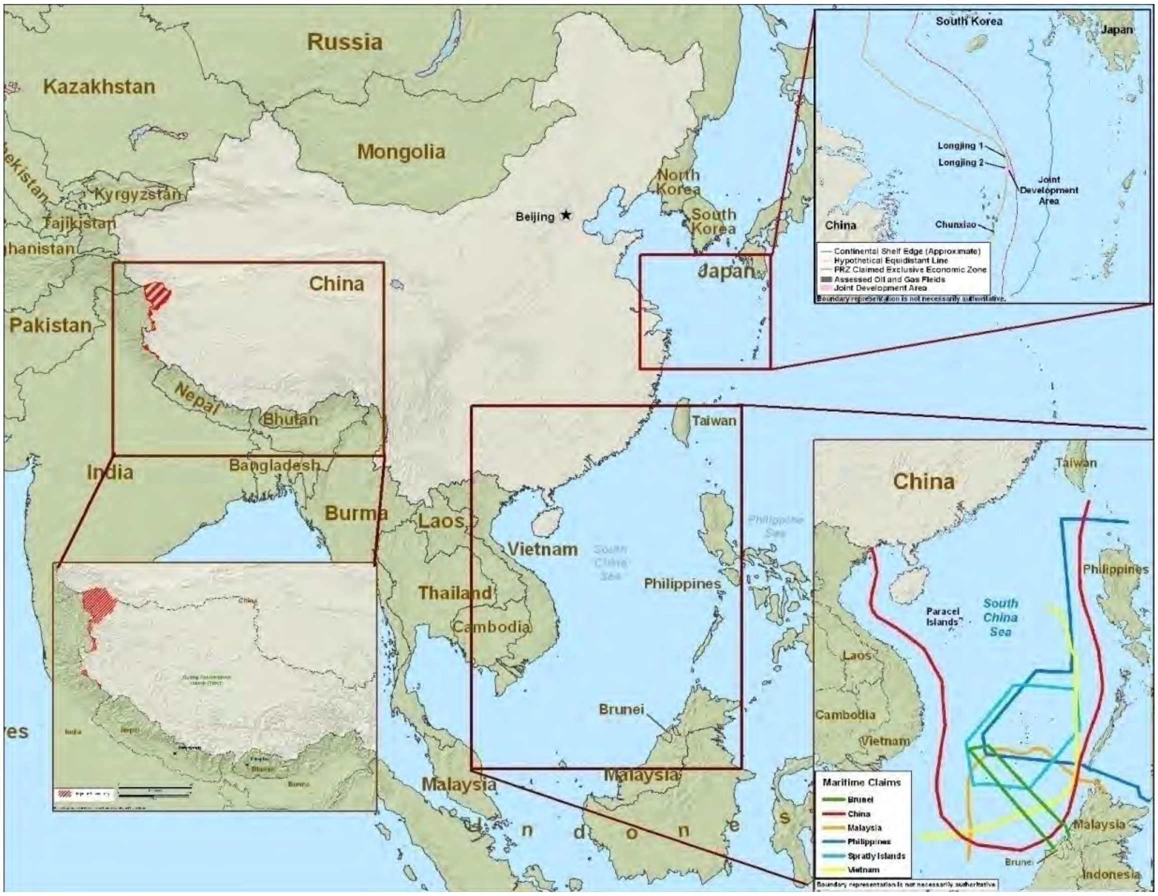

Figure 3. China‘s Historical Claims and Disputed Territories
Source: Office of the Secretary of Defense, —Military and Security Developments Involving the People‘s Republic of China 2010,” *Annual Report to Congress* (Washington, DC: Government Printing Office, 2010), 16.

There can be no mistaking China‘s intent to —win local wars under the conditions of informationization."[56] China sees the —informationization" of society as inevitable and cyber space as a new strategic domain.[57] Stated repeatedly in China‘s 2010 National Defense white paper is the need to develop joint operations, joint operation systems, and training under, —conditions of informatization."[58] This extends to recruiting talented people and developing new types of combat forces, then integrating them with civilian enterprises.[59] These talented people are information technology specialists and experts with —improved ideological and political qualities."[60] China considers this dramatic change of combining civilian-military development in a world of informationization, —a revolution in military affairs with Chinese characteristics."[61]

Combining the three concepts of defense for defensive purposes only, the modernization of forces to deter, fight, and defeat enemies in cyber space, and the peaceful rise of China in reclaiming its former glory, presents an interesting perspective into China‘s strategy. Why would China modernize a military used for defensive purposes only? The answer to that comes from the former Soviet Union. The fall of the Soviet Union stressed an important point that entering into an arms race with the U.S. is counterproductive to economic expansion and ultimately futile.[62] Developing a defensive capability can be less expensive but only in the context of fighting local wars. The capability to project military power or defend distant lands becomes more difficult and expensive the longer the lines of communication become. Secondly, conducting offensive military operations might jeopardize world opinion that China‘s rise to power is peaceful in nature. This in turn would harm China‘s goal of restoring its former glory. Lastly, China may not envision engaging in war in other countries, as exemplified by —windcal wars,” and therefore can focus on national defense for defensive purposes rather than offensive expansionist purposes. This does not mean China is not pursuing offensive capability rather that the current focus of the military is more defensive.

Lessons learned from the 1991 Gulf War, propelled China down a path of modernization with ―informationization” as the impetus.[63] This modernization led to the development cyber theory, doctrine, and new organizations. However, the realm of cyber space does not equate to purely defensive capabilities. Clearly, both offensive and defensive capabilities are possible in cyber space and as mentioned earlier, China has the capability to do both.

This is what the Chinese call an active defense. The concept of the active defense is a defense in depth approach at the tactical, operational, and strategic levels of war.[64] The idea is to attack selected key nodes through the, ―integration of available strength” with the, ―integrated application of techniques.”[65] The integration of available strength brings together the capabilities of forces operating in the domains of land, air, sea, space, and cyber space for synergistic effect. The integration of techniques is effects-based and combines the use of destructive and disruptive methods.[66] An application of the active defense in cyber space would target an enemy‘s computer networks for destruction or disruption while protecting one‘s own.

Recent Activities

There is no shortage of circumstantial evidence that China is actively participating in or sponsoring malicious cyber activity around the world. Canada, the U.S., India, and Iran are a small sample of countries accusing China of hacking or cyber espionage. There is little doubt that servers used in perpetrating these attacks are located in China. Forensic analysts from the Information Warfare Monitor discovered four such servers used by GhostNet in the collection of electronic documents, email, and address lists. China denies any involvement in such activity stating that such accusations are —groundless” and have —ulterior motives.”[67] In a majority of these cases, China‘s statements may have some validity as hacker groups say they act of their own accord. One problem for the victims of malicious cyber activity is the lack of cooperation from the Chinese government in finding those responsible. This perceived stalling or dismissal of requests to find those responsible creates suspicion that the Chinese government either is involved or condones such activity.

Recently two cyber events, the infiltration of Google‘s networks in 2010 and a similar event of an unnamed company reported by Northrop Grumman in a 2009 report to the U.S.-China Economic and Security Review Commission suggest state involvement. While these events were separate incidents, the attack on Google and the unnamed company share many similar forensic characteristics. In each case, the hackers had access to the most sophisticated hacking tools available, utilized a team approach by designating responsibility for access, reconnaissance, and exfiltration of data. Further, Chinese is the language for much of the hacking software code and the servers used in conducting the attacks are located in China. While circumstantial evidence suggests the Chinese government is complicit in these events, attribution in cyber space is virtually impossible with today‘s investigative techniques.

The software used in hacking the networks was highly sophisticated. It is possible that an individual hacker could develop such software but realistically it requires some level of research. China openly states they are pursuing the integration of military and civilian development to include business and academia. This integration would provide the required facilities to develop software and the infrastructure to utilize it. Tim Thomas notes that the two servers used in the attacks on Google are located at Shanghai Jiaotong University and Lanxiang Vocational School. Lanxiang is a high school level education facility with a computer laboratory so large it is in the *Guinness Book of World Records* as having the largest computer class in one location. Jiaotong University also has a school of Information Security Engineering and direct ties to the PLA.[68] Headed by the former director of China‗s foreign intelligence service, Jiaotong University lists a former hacker with a specialty in CNE as an affiliated researcher.[69]

Regarding the team approach, the Northrop Grumman report details the use of two teams, one team to breach network security, and a second team to collect the desired data.[70] In the Google incident, it appears that a single coordinated team conducted the attack. The Northrop Grumman example does not provide specific dates when the attack occurred saying only, ―several years ago."[71] The attack could have taken place at any time but the wording suggests that it was sometime around 2006 or 2007 and the Google attack occurred in January 2010. The use of separate teams is consistent with the organization of the 3rd and 4th General Staff Departments at that time with one team conducting reconnaissance, 3rd GSD, and the other team conducting attack, 4th GSD. In 2008, it appears that all CNO became the purview of the 4th GSD and the IW militia unit organization changed adding CNE and CND elements to the unit. This organization is consistent with the single team approach used in the attack on Google.

History, Culture, Politics, and Religion

Beginning with the Opium Wars and ending with the creation of the Chinese Communist Party, China saw a steady decline of national power. The CCP maintains that China suffered the insults of imperial powers imposing their will on Chinese society for a, ―century of national humiliation."[72] To the Chinese this period was a great embarrassment and reflected poorly on the Chinese people, society, and the nation. In an effort to restore national pride, China developed the goals of reclaiming former territories, enhancing regional influence, deterring aggression against China, defending sovereign territory, and improving international stature.[73]

With these principles in mind, China set itself on a course first seeking to reclaim areas it considers as sovereign territory. The first territory that comes to mind is Taiwan and this example is perfectly illustrates China‘s ever evolving strategic vision. Since 1955, China has tried several different tactics in reuniting Taiwan with mainland China. The use of force against Taiwan in 1955 and again in 1958 might have succeeded if not for U.S. intervention on each occasion. The tactic changed to a show of force by conducting military exercises in the Strait of Taiwan as happened in 1996 or with the test firing of a new missile in 2000.[74] More recently, China has switched its approach from the use of _sticks‘ to _carrots‘ by opening travel, mail, and trade with Taiwan. The change over time in China‘s approach toward Taiwan provides an excellent illustration of China‘s continual evolution in strategic thinking. China recognizes that pursuing its national goals through economic means is slower than the use of military force but this method positively affects international stature, regional influence, and with a secondary benefit of deterring aggression against China. This change in strategic approach is in line with the new security concepts of mutual trust and mutual benefit, and that the country‘s overall development is the highest priority.[75] In spite of this approach, China steadfastly maintains the right to use military force against Taiwan if the Taiwanese government should openly declare independence from China.[76]

Strategy dates back in time as far as China itself. The teachings of Sun Tzu, Confucius, Chinese proverbs, and the combined wisdom of the 36 stratagems are unique to Chinese culture. In general, much of what these writings offer is an understanding of how to think rather than what to think.[77] These lessons are not specific solutions to a specific problem. Rather the intent is to communicate a philosophy to the reader allowing them to develop a higher level of learning and the ability to define new problems in old ways. To understand this further, it is important to understand the symbolism and the cultural connection to it. One such symbol is the unity of opposites represented by yin and yang.[78]

Yin and yang divide the world into two categories, where each element in yin is the complete opposite of each element in yang. Yin is light and yang is dark. Yin is water and yang is fire. Yin is female and yang is male. Every element in yin is paired with an opposite element in yang and one cannot exist without the other. This is the philosophy of *I Ching,* the unity of opposites. In Chinese culture, stratagems belong to yin.[79] Stratagems differ from strategy. A stratagem is a plan of deception devised to gain an advantage over an adversary. There are 36 stratagems in Chinese culture and they provide the concepts of using deception coupled with the philosophy of opposites. An example is, ―pretend to take one path while sneaking down another.”[80] Gao Yuan describes this stratagem best, highlighting both deception and opposites, saying, —[T]his stratagem plays overt, predictable, and public maneuvers against covert, surprising, and secretive ones.”[81]

The unity of opposites appears throughout the 36 stratagems as well as Sun Tzu‘s writings. Samuel Griffith‘s introduction in *The Art of War* identifies cheng and ch‘i as the direct or fixing force and the indirect or encircling force respectively.[82] The concept of ch‘i and cheng are very much alike in the same way that yin is to yang. In the examples from Sun Tzu, —when capable, feign incapacity; when active, inactivity.”[83] Another way of stating this stratagem is to appear weak when strong, and strong when weak. In the unity of opposites, one element can change or transform into its opposite where weak becomes strong or an attack becomes a defense.[84] This stratagem helped to develop China‘s strategy on informationization by turning the American strength of managing battlefield information into a weakness through the exploitation of the heavy reliance on C4ISR systems.

The unity of opposites explains what Sun Tzu writes regarding the use of deception. Sun Tzu states twice that, —all warfare is based on deception.”[85] Deng Xiaopeng reflects this mode of thinking in his 24 Character Strategy. Deng writes, —observe calmly; secure our position; cope with affairs calmly; hide our capacities and bide our time; be good at maintaining a low profile; and never claim leadership.” Analyzing this statement through the lens of the unity of opposites clarifies and brings China‘s intent into focus. Deng is communicating with the Chinese people in a way that even if subconscious, is familiar to them. Words like low profile and leadership are opposites. The hiding of capacities is the warfare of deception.

This concept easily transfers to what Westerners perceive as incongruities between China's statements and their actions. Officially Chinese law prohibits all forms of hacking, yet the PLA officially sanctions and sponsors hacking competitions. Countries claiming that cyber attacks originated in China receive only statements of official policy and counter accusations but no assistance in ferreting out the perpetrators. China is very comfortable dealing with deception and explaining seemingly opposing views in the same sentence.

In China, it is impossible to separate the activities of the government from those of the Communist Party. Members of the government hold key leadership positions in the Party and within the PLA. More appropriately, Party members hold office in the government and the military. As such, the Party controls both the government and the PLA and implements its brand of ideology on the people. The reason for this duplicity of control is to maintain the power and dominance of the Communist Party.[86] The CCP has shown on several occasions that the preeminence of the party maters more than anything else. A good example of this was the student demonstrations in Tiananmen Square and the CCPs use of deadly force against peaceful demonstrators.

China's 2010 Defense white paper sums up the events of Tiananmen Square the best. The PLA has the critical task of maintaining the overall social stability of the nation while supporting the government.[87] Social stability equates to the CCPs ability to control the people through policy, laws, psychology, public opinion, or military force and has little to do with the happiness of the people. Tiananmen Square is the concept of the ―three warfares" in action 14 years before its official publication. China justifies the killing of peaceful demonstrators by using the media to portray them as subversives and a threat to social stability. China also denounced foreign criticism as intervention in China‘s internal affairs. They used Chinese laws and regulations as further justification for the use of deadly force. In April 1989, about two months before the use of force, Secretary General Ziyang Zhao expressed his sympathies toward the students. Deng immediately called Zhao a traitor and had him placed under house arrest.[88] The CCP officially declared martial law on May 20th and ordered nearly 300,000 soldiers, including an armored division and an airborne division, to Beijing.[89] Late on the evening of June 3rd, the PLA rolled into Tiananmen Square using tanks and machine guns to run over and kill the demonstrators. The events surrounding Tiananmen Square show that the CCP will resort to extreme measures to remain in control using the need to maintain social stability as an excuse.

The idea of a single entity in complete control of China was not born out of the communist revolution. This idea dates back thousands of years to the earliest emperors and known as the mandate of heaven. The mandate simply states that those in power do so by the will of heaven alone and the power to rule lasts only as long as the actions of the ruler pleases heaven. The mandate further states that there can be only one ruler. Today, the CCP uses the mandate to justify its position of authority explicitly.

Internal and External Threats

China‘s 2010 National Defense white paper lists Taiwan, Tibet, and East Turkistan, also known as Xinjiang province, as areas presenting a security concern. Specifically, China states that, —separatist forces have inflicted serious damage on national security and social stability.”[90] The defense policy has three main goals of, —resisting foreign aggression, defending the motherland, and safeguarding social stability."[91] From this statement, internal and external threats classify as either the subversion of social stability or foreign aggression. It cannot be emphasized enough the importance China places on social stability. The PLA has the critical task to maintain social stability and, ―to subdue all subversive and sabotage activities."[92] Social stability is the generic phrase used by the CCP to arbitrarily determine who or what is a threat. In this case, the definition of threat is an individual, group, or organization that speaks out against the CCP, its ideology, or its policies.

[1] Menges, 83.

[2] Dreyer, 285.

[3] The World Bank, http://data.worldbank.org/indicator/NY.GDP.MKTP.CD (accessed 27 April 2011).

[4] U.S. Department of State, http://www.state.gov/r/pa/ei/bgn/18902.htm (accessed 3 May 2011).

[5] Jeffrey Richelson and Michael Evans, ―Tiananmen Square, 1989: The Declassified History," (1 June 1999), http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB16/documents/index.html#f1 (accessed 5 May 2011).

[6] Ibid.

[7] U.S. Department of State.

[8] U.S. Department of State; Menges, 112.

[9] Menges, 113.

[10] Ibid., 114.

[11] Dreyer, 285-286.

[12] Ibid., 286-287.

[13] Menges, 116.

[14] Dreyer, 287-288.

[15] Dreyer, 286-287; Menges, 120-121.

[16] Menges, 121.

[17] Dreyer, 287-288.

[18] Menges, 121.

[19] Dreyer, 289.

[20] Menges, 121.

[21] OSD, —Military Power of the People‘s Republic of China," 11.

[22] Ibid.

[23] Ibid.

[24] Ibid., 13.

[25] Deepak Sharma, —Integrated Network Electronic Warfare: China‘s New Concept of Information Warfare," *Journal of Defence Studies* 4, no. 2 (April 2010): 38-39, http://www.idsa.in/system/files/jds_4_2_dsharma.pdf (accessed 12 May 2011).

[26] Krekel, 15.

[27] Ibid.

[28] Ibid.

[29] Ibid.

[30] Krekel, 15; Bartholomew, 171.

[31] Krekel, 15.

[32] Ibid., 32.

[33] Ibid.

[34] Ibid., 33.

[35] Ibid., 36.

[36] OSD, —Military and Security Developments Involving the People‘s Republic of China 2010," 26.

[37] Cheng, —China‘s Active Defense Strategy and its Regional Impact," 4.

[38] Krekel, 36.

[39] Ibid., 34.

[40] Ibid.

[41] Krekel, 37.

[42] Henderson, 126.

[43] Ibid., 126-129.

[44] Ron Deibert, and Rafal Rohozinski, ―Tracking GhostNet: Investigating a Cyber Espionage Network," *Information Warfare Monitor Joint Report 02-2009* (Toronto, Canada: 29 March 2009), 1.

[45] Ibid., 48.

[46] Henderson, 69.

[47] Ibid., 128.

[48] Ibid.

[49] Holly Williams, ―China‘s Cyber Hackers Target Western Firms," *Skynews*, 18 April 2011, http://news.sky.com/skynews/Home/World-News/Video-Chinas-Cyber-Hackers-Growing-Threat-To-Western-Security-Sky-News-Investigation/Article/201104315974328?lid=ARTICLE_15974328_Video:ChinasCyberHackersGrowingThreatToWesternSecuritySkyNewsInvestigation&lpos=searchresults (accessed 16 May 2011).

[50] Timothy Thomas, ―Google Confronts China‘s Three Warfares," *Parameters* 40, no. 2 (2010): 105-106.

[51] OSC, ―China‘s National Defense in 2010."

[52] Ibid.

[53] Ibid.

[54] Ibid.

[55] Ibid.

[56] Ibid.

[57] Ibid.

[58] Ibid.

[59] Ibid.

[60] Ibid.

[61] Ibid.

[62] Dreyer, 290.

[63] OSC, —China‘s National Defense in 2010.”

[64] Cheng, —China‘s Active Defense Strategy and its Regional Impact,” 1-2.

[65] Ibid., 2.

[66] Ibid., 3.

[67] Elegant, —Enemies at the Firewall.”

[68] Thomas, —Google Confronts China‘s Three Warfares,” 104-105.

[69] Krekel, 48.

[70] Ibid., 61.

[71] Ibid., 59.

[72] Larry Wortzel, —China‘s Foreign Conflicts Since 1949,” in *A Military History of China,* ed David A. Graff, Robin Higham (Boulder, CO: 2002), 270.

[73] Ibid.

[74] Ibid., 268.

[75] OSC, —China‘s National Defense in 2010.”

[76] Maxcy, —China‘s Military Art, Wars, and Revolution.”

[77] Yuan, 16.

[78] Ibid., 17.

[79] Ibid.

[80] Ibid., 60.

[81] Ibid.

[82] Sun Tzu, *The Art of War*, trans. by Samuel B. Griffith (New York, NY: Oxford University Press, 1971), 42.

[83] Ibid, 66.

[84] Yuan, 17; Sun Tzu, 42.

[85] Sun Tzu, 66.

[86] Menges, 369.

[87] OSC, ―China‘s National Defense in 2010.”

[88] Menges, 108-110.

[89] Ibid., 110.

[90] OSC, ―China‘s National Defense in 2010.”

[91] Ibid.

[92] Ibid.

CHAPTER 5

CONCLUSIONS AND RECOMMENDATIONS

Conclusions

Beginning in the early 1990s, China determined that in order to achieve global influence and parity with the U.S., they must expand their economy by implementing Deng‘s economic reforms. Economic expansion became the means for China‘s return to international prominence, prosperity, and influence. Economic growth is the foundation that allows China to pursue all other improvements and reforms, particularly the modernization of the PLA. Simultaneously with the economic reforms, China conducted a full-scale comparison of the PLA capabilities to the U.S. military performance in the 1991 Gulf War. This comparison highlighted the inadequacies of the PLA to conduct warfare and manage battlefield information with the same capabilities and level of proficiency as the United States. Over a period of five years the PLA developed the concept of informationization and began the process of determining how this could become a reality. The first step toward achieving informationization was the establishment of the Technical Reconnaissance Bureaus. The bureaus were the initial proof of concept and helped to further China‘s understanding of how to use the cyber domain to achieve their national objectives.

Based on the lessons learned from the reconnaissance bureaus, General Dai developed China‘s initial information warfare doctrine and the control of the electromagnetic spectrum. Dai continued to refine his doctrine, incorporating electronic warfare with network attack leading the PLA to adopt INEW as the official doctrine. For his work, Dai was promoted to lead the 4th GSD with the responsibility for EW and

CNA. It is not clear if Dai‘s doctrine led to the development of the first IW militia unit or if these events happened simultaneously, however, the unit became a second proof of concept and represents the further development of China‘s thinking toward cyber warfare. The PLA initially recruited members for the unit that were extremely loyal to the CCP and had the necessary technical skills. By locating the unit in the information technology center of Guangdong province, the IW militia unit capitalized on the readily available infrastructure, personnel, and technology.

Initially, the IW units concentrated their efforts on the further development of network attack, but the risks associated with conducting such activities outside China‘s national borders and combined with the lack of well-defined international standards establishing redlines of what constitutes cyber warfare resulted in the PLA diversifying the unit capabilities to include network reconnaissance and defense. This move incorporated all computer network operations into a multi-functional unit with oversight provided by the 4th GSD. Further, the PLA created six more IW militia units and assigned each unit to a military region providing the regional commanders with a CNO capable unit. The Central Military Commission controls the direction of the IW units operations through the military chain of command and resources the unit through the direct partnership with industry.

The IW militia units conduct their training by executing network attack against opposition forces networks during military exercises. This training provides the IW unit with the needed experience of how to effectively disrupt information and disable an adversary‘s networks while simultaneously creating a degraded information environment for friendly units to train in what China considers as the operating environment of future conflict. More importantly than training on network attack, the IW militia units need to train on network exploitation. Network exploitation is the most difficult of all network operations. Hacking into government or military networks without the knowledge of the network security managers is not an easy task. Only organizations with the most sophisticated hacking software, access to the latest technology, and the best technical support are capable of conducting exploitation without detection. Such operations provide detailed network information necessary for conducting network attack and extracting technology information used in modernizing military equipment. The IW militia units have the capability to conduct all forms of CNO, trains using the INEW doctrine, has the support of the state, and direct access to technology, software, and experience making them the most likely means to achieve the goals of China‘s national strategy.

Officially, China stresses the need to maintain social stability and tasks the PLA to ensure that this occurs. Tibet, Taiwan, and Xinjiang province conflict with the CCPs definition of social stability by calling for independence and autonomy, which is a threat to the dominance of the Party. The IW militia units provide the unique capability to the CCP by maintaining control without resorting to the traditional use of the military force. Incidents like Tiananmen Square draw immediate negative reactions from the international community with corresponding sanctions against China. Contrary to this, the use of the cyber domain to block or restrict opposition group collaboration and monitoring their activities draws little notice. The use of the Internet as a means to connect to foreign markets and create economic expansion is also a necessary tool to maintain social stability. The danger lays in the possible injection of unwanted information, particularly American democratic influence, into Chinese society. Domestically, China views American values as a serious threat influencing the actions of dissidents in an attempt to overthrow the CCP. As such, China‘s Internet policy restricts access to opposition websites and Internet providers closely monitor all Internet traffic. In this environment, Tibet, Taiwan, and Xinjiang are domestic threats, while the U.S. is an international threat.

The international community attributes many acts of cyber espionage to China based on forensic analysis determining the location of servers used in the attacks and the programming language. In each case, China vehemently denies any involvement arguing that Chinese laws prohibit such activity however; China has not been forthright in working with other nations to discover who might be behind such attacks. Attribution of cyber attacks is virtually impossible with current technology and prevents an accuser from providing incontrovertible evidence. Under this cloud of uncertainty, China can conduct extensive CNO against foreign governments, militaries, and opposition groups to collect all types of information. Sometimes this information is collected in massive amounts exemplified by the rerouting of 17 minutes of Internet traffic through Chinese servers. At other times, the information is very specific such as the Joint Strike Fighter program and requires years to infiltrate and map the network before extracting the information.

China‘s history dates back thousands of years. During this time, China has witnessed the rise and fall of their civilization. At the end of thousands of years of dynastic rule, foreigners pressed China into opening trade routes with the West. Militarily, China was weak and unable to prevent Westerners from making demands and exacting lopsided trade agreements. For the period of 100 years, China suffered the national humiliation of foreign occupation in economic exclusion zones. The rise of the Chinese Communist Party in 1949 ushered in a new era of China‘s return to the former glory and power of the Middle Kingdom. After years of occupation and loss of historical territories to Russia, Britain, France, and Japan, China began the task of reclaiming these territories and disputed lands. Over time, China‘s approach to reclaiming these lands has gradually switched from the use of military force to economic incentives but the ultimate goal remains the reunification of all sovereign lands under the banner of the CCP. The reunification of Taiwan into the PRC and subsequent U.S. intervention and support of Taiwan remains an open sore to the Chinese government. China is willing to use economic influence to regain Taiwan but openly states that the use of military force remains an option.

Finally, China‘s INEW doctrine combining network attack with electronic warfare supports the use of cyber warfare in future conflict. The IW militia unit organization provides each Chinese military region commander with unique network attack, exploitation, and defense capabilities. IW unit training focuses on improving network attack skills during military exercises. The integration of the IW militia units with commercial technology companies provides infrastructure and technical support enabling the units to conduct operations. The IW units gather intelligence on an adversary‘s networks identifying critical nodes and security weaknesses. Armed with this intelligence, these units are capable of conducting network attack to disrupt or destroy the identified critical nodes of an enemy‘s C4ISR assets allowing China to use military force in a local war. In an effort to regain its former status, China pursues the strategic goal of reunification of its claimed sovereign territories and lands using economic influence as the primary means but will resort to military force if necessary. Recent cyber activities attributed to China suggest that network exploitation is currently underway and providing military, political, and economic information to the CCP. Domestically and internationally, China views Taiwan and the United States respectively, as the major threats to the CCP. Cyber warfare is a significant component of China‘s national strategy domestically to promote social stability and internationally to disrupt or delay foreign military intervention in China‘s internal affairs.

China‘s cyber capabilities support the ends of China‘s national strategy by exploiting America‘s heavy reliance on networked information systems through deception, deterrence, and reconnaissance. The combined actions of pursuing a modernized military force capable of conducting local wars under informatized conditions with the development of doctrine, units, training, and resources show China‘s commitment to achieving dominance in cyber space as a means to achieving their national strategic goals. Recent cyber activities suggest that China is conducting network exploitation to gather information on military, government, and commercial networks inside the United States. Using the concept of ―three warfares,” China utilizes the media, psychological, and legal means to deceive and deter the U.S. from intervention in China‘s internal affairs such as Taiwan or Tibet. In the event that Taiwan declares independence from China, China is likely to use the information gathered on U.S. C4ISR networks temporarily disabling America‘s information management capability with limited cyber attacks. These attacks will delay U.S. military intervention using conventional forces long enough for China‘s conventional forces to secure Taiwan. Reunifying Taiwan with mainland China would reduce the U.S. presence in East Asia and further China's aim of controlling their claimed sovereign territory.

The significance of this study relates to the relevance of cyber warfare and the need to control the cyber domain in future conflict. While it is sometimes difficult to comprehend the technical aspects of cyber space as well as its lack of physical dimensions, cyber space provides unique opportunities for advancing national interests through collaboration and the sharing of information, economic expansion, and cooperation. Simultaneously, cyber space represents a domain of warfare providing enemies avenues to exploit and attack networks to achieve information dominance.

Recommendations

China has the capability to penetrate the networks of the United States government, military, and commercial firms. Therefore, the U.S. should implement the following recommendation to mitigate risk and possibly prevent such attacks. The U.S. should lead the international community in establishing an international protocol regarding the use of cyber space for peaceful and defensive purposes only. Such an agreement would lessen the likelihood of cyber space becoming a new medium for an electronic arms race and would provide assurances to signatories wanting to take advantage of cyber space for domestic economic growth.

Recommendations for Further Study

This study shows that China is conducting network exploitation but it is difficult to determine if the exploitation meets the criteria U.S. government officials consider an act of war. Further study is needed to determine when network exploitation becomes an act of war. With no clear definition, international standards, or U.S. redlines on cyber warfare, the study of this topic would provide useful information to political and military leaders and improve overall knowledge of cyber operations. Additionally, cyber espionage, particularly of defense industry corporations, requires further study. As China continues its pursuit of economic and military parity with the U.S., the stealing of trade secrets and technologies from U.S. firms remains the fastest way of achieving that goal.

BIBLIOGRAPHY

Books

Dreyer, June Teufel. —Recent Developments in the Chinese Military." In *A Military History of China,* edited by David A. Graff and Robin Higham, 285-302. Boulder, CO: 2002.

Gertz, Bill. *The China Threat: How the People's Republic Targets America.* Washington, DC: Regenery, 2000.

Henderson, Scott J. *The Dark Visitor: Inside the World of Chinese Hackers*. Fort Leavenworth, KS: Foreign Military Studies Office, 2007.

Menges, Constantine. *China: The Gathering Threat*. Nashville, TN: Nelson Current, 2005.

Mosher, Steven W. *Hegemon: China's Plan to Dominate Asia and the World*. San Francisco, CA: Encounter Books, 2000.

Nye, Joseph S. Understanding International Conflicts: An Introduction to Theory and History. 7th ed. Boston, MA: Pearson Longman, 2009.

Qiao, Liang, and Wang Xiangsui. –Unrestricted Warfare." In *Air War College Nonresident Studies Senior Leader Course Book 5*, edited by Elice Lindsey-Isome, 341-378. Maxwell Air Force Base. AL: Government Printing Office, 2006.

Thomas, Timothy L. *Decoding the Virtual Dragon*. Fort Leavenworth, KS: Foreign Military Studies Office, 2007.

———. *Dragon Bytes: Chinese Information War Theory and Practice*. Fort Leavenworth, KS: Foreign Military Studies Office, 2004.

———. *The Dragon's Quantum Leap*. Fort Leavenworth, KS: Foreign Military Studies Office, 2009.

Tzu, Sun. *The Art of War*. Translated by Samuel B. Griffith. New York, NY: Oxford University Press, 1971.

Wortzel, Larry. —China's Foreign Conflicts Since 1949." In *A Military History of China,* edited by David A. Graff and Robin Higham, 267-284. Boulder, CO: 2002.

Yuan, Gao. *Lure the Tiger Out of the Mountains: The 36 Stratagems of Ancient China*. New York, NY: Simon and Schuster, 1991.

Periodicals

Cheng, Dean. —Chinese Views on Deterrence” *Joint Force Quarterly* no. 60 (1st Quarter 2011): 92-94.

Clayton, Mark. —China Cyber Attacks: Google only one of many US Targets.” *The Christian Science Monitor* (January 2010). http://www.csmonitor.com/USA/ 2010/0113/China-cyber-attacks-Google-only-one-of-many-US-targets (accessed January 2011).

The Economist. —Marching Off to Cyberwar.” 4 December, 2008. http://www.economist. com/node/12673385?story_id=12673385 (accessed 26 April 2011).

Elegant, Simon. —Enemies at the Firewall.” *Time*, December 2007. http://www.time.com/ time/magazine/article/0,9171,1692063-1,00.html (accessed 26 April 2011).

Gorman, Siobhan. —Electricity Grid in U.S. Penetrated by Spies.” *Wall Street Journal*, 8 April 2009. http://online.wsj.com/article/SB123914805204099085.html (accessed 22 February 2011).

Keymer, Elanor. —AnalysisIs the Threat of Cyber Attack Overblown?” *Jane's Defence Weekly* (20 January 2011).

McMillan, Robert. —Was Stuxnet Built to Attack Iran‘s Nuclear Program?” *PCWorld,* 21 September 2010. http://www.pcworld.com/businesscenter/article/205827/ was_stuxnet_built_to_attack_irans_nuclear_program.html (accessed 30 March 2011).

Newmyer, Jaqueline. —The Revolution in Military Affairs with Chinese Characteristics.” *The Journal of Strategic Studies* 33, no. 4 (August 2010): 483-504. http://www.informaworld.com/smpp/section?content=a926059415&fulltext=713240928#references (accessed 26 April 2011).

Ophardt, Jonathan A. —Cyberwarfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow‘s Battlefield.” *Duke Law and Technology Review* (February, 2010). http://www.law.duke.edu/journals/dltr /articles/ 2010dltr003.html#B19 (accessed 26 April 2011).

Skinner, Tony. —War and PC: Cyberwarfare.” *Jane's Defence Weekly* (19 September 2008).

Stevens, Tim. —Breaching Protocol- the Threat of Cyberespionage.” *Jane's Intelligence Review* (11 February 2010).

Thomas, Timothy L. —Google Confronts China‘s _Three Warfares‘.” *Parameters* 40, no. 2 (Summer 2010): 101-113.

Government Documents

Badoud, Thomas, Frank Carapezza, Hilary Clark, Kathryn Cubbon, Tim Deerr, Sara DeWitz, Chris Fraser, Jessica Rocha, James Stanley, Jon Stevenson, and Laresa Walter. *Targeting U.S. Technologies: A Trend Analysis of Reporting from Defense Industry, 2010*. Washington, DC: Government Printing Office, 2010.

Bartholomew, Carolyn. *2009 Report to Congress of the U.S.-China Economic and Security Review Commission*. Washington, DC: Government Printing Office, 2009.

Chairman of the Joint Chiefs of Staff. Joint Publication (JP) 3-13, *Information Operations.* Washington, DC: Government Printing Office, 2006.

Information Office of the State Council. *China's National Defense in 2010*. Beijing, China: Xinhua News Agency, 2011. http://www.chinadaily.com.cn/ china/2011-03/31/content_12256413.htm (accessed 3 April 2011).

———. *The Internet in China*. Beijing, China: Information Office of the State Council, 2010. http://www.china.org.cn/government/whitepaper/2010-06/08/ content_20208007.htm (accessed 20 April 2011).

Krekel, Bryan. *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*. Prepared for the US-China Economic and Security Review Commission. McLean, VA: Northrup Grumman Corporation, 2009.

Office of the Secretary of Defense. *Annual Report to Congress: Military Power of the People's Republic of China.* Washington, DC: Department of Defense, 2007.

———. *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China*. Washington, DC: Department of Defense, 2010.

Slane, Daniel M. *2010 Report to Congress of the U.S.-China Economic and Security Review Commission.* Washington, DC: Government Printing Office, 2010.

U.S. Army Training and Doctrine Command (TRADOC). Field Manual (FM) 3-13, *Information Operations: Doctrine, Tactics, Techniques, and Procedures.* Washington, DC: Government Printing Office, 2003.

———. Pamphlet 525-7-8, *Cyber Space Operations Concept Capability Plan 2016-2028*. Washington, DC: Government Printing Office, 2010.

———. Field Manual (FM) 1-02, *Operational Terms and Graphics.* Washington, DC: Government Printing Office, 2004.

Wortzel, Larry. —China‟s Approach to Cyber Operations: Implications for the United States." Testimony before the Committee on Foreign Affairs Hearing on —The Google Predicament: Transforming U.S. Cyberspace Policy to Advance Democracy, Security, and Trade." Washington, DC: Government Printing Office, 2010.

Other Sources

Adair, Steven, Ron Deibert, Rafal Rohozinski, Nart Villeneuve, and Grag Walton. *Shadows in the Cloud: Investigating Cyber Espionage 2.0*. Toronto, Canada: Information Warfare Monitor, April, 2010.

Brookes, Peter. *China's Cyber Spies*. http://www.heritage.org/Research/Commentary/2008/11/Chinas-Cyber-Spies (accessed 26 April 2011).

Carafano, James. *Obama Needs to Address Our Cyber-Warfare Gap with China*. http://www.heritage.org/Research/Commentary/2011/01/Obama-Needs-to-Address-Our-Cyber-Warfare-Gap-with-China (accessed 27 April 2011).

Cheng, Dean. *China's Active Defense Strategy and Its Regional Impact*. http://www.heritage.org/Research/Testimony/2011/01/Chinas-Active-Defense-Strategy-and-Its-Regional-Impact (accessed 26 April 2011).

———. *China's Indian Provocations Part of Broader Trend*. http://www.heritage.org/Research/Reports/2010/09/Chinas-Indian-Provocations-Part-of-Broader-Trend (accessed 26 April 2011).

———. *China and Cyber Security*. http://www.heritage.org/Events/2010/04/China-and-Cybersecurity (accessed 26 April 2011).

Consulate General of the People‘s Republic of China. http://houston.chinaconsulate.org/eng/nv/t140964.htm (accessed 3 March 2011).

Deibert, Ron, and Rafal Rohozinski. *Tracking GhostNet: Investigating a Cyber Espionage Network*. Toronto, Canada: Information Warfare Monitor, March 2009.

Eckert, Paul. *China Military Build-up Seems U.S. Focused*. http://uk.reuters.com/article/2009/05/04/us-usa-china-military-idUKTRE54363X20090504 (accessed 26 April 2011).

Friedman, Thomas. —National Strategies and Capabilities for a Changing World: Globalization and National Security." In C100, *Foundations,* Department of Command and Leadership, 81-95. Fort Leavenworth, KS: Government Printing Office, 2010.

Fritz, Jason. ―How China will use cyber warfare to leapfrog in military competitiveness." *Culture Mandala: The Bulletin of the Centre for East-West Culture and Economic Studies* 8 no. 1 (October 2008): 33-39. http://epublications.bond.edu.au/cm/vol8/iss1/2 (accessed 11 May 2011).

Hooker, Richard. ―Ch‘ing China: The Opium Wars." http://www.wsu.edu:8080/~dee/CHING/OPIUM.HTM (accessed 20 April 2011).

———. ―Ancient China: The Chou." http://www.wsu.edu:8080/~dee/ANCCHINA/ANCCHINA.HTM (accessed 20 April 2011).

———. ―Ch‘ing China: The Boxer Rebellion." http://www.wsu.edu:8080/~dee/CHING/BOXER.HTM (accessed 20 April 2011).

Langner, Ralph. ―Cracking Stuxnet, a 21st-century cyber weapon." http://www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyberweapon.html (accessed 30 March 2011).

Lee, John. ―China‘s American Obsession: Why Osama bin Laden‘s Death is Making Chinese Leaders Nervous." http://www.foreignpolicy.com/articles/2011/05/06/china_s_america_obsession?page=0,0 (accessed 9 May 2011).

Leydon, John. ―EU Parliament Suspends Webmail after Cyber-attack." *The Register*, 31 March 2011. http://www.theregister.co.uk/2011 /03/31/eu_parliament_hack (accessed 3 April 2011).

Ljunggren, David. ―Canada Says Cyber-attack Serious, Won‘t Harm Budget." *Reuters,* 17 February 2011. http://www.reuters.com/ article/2011/02/17/us-cyberattack-idUSTRE71G0RG20110217 (accessed 3 April 2011).

Maxcy, William. ―ChinaMilitary Art, Wars, and Revolution." Lecture in U.S. Army Command and General Staff College, March 2011, Fort Leavenworth, KS.

Miller, Joshua Rhett. ―Internet Traffic from U.S. Government Websites was Redirected Via Chinese Networks." *Foxnews*. http://www.foxnews.com/politics/2010/11/16/internet-traffic-reportedly-routed-chinese-servers/ (accessed 5 March 2011).

Obama, Barak. ―Remarks by the President on Securing Our Nation‘s Cyber Infrastructure." Washington, DC: The White House, 2009. http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/ (accessed 3 March 2011).

Reuters. *China's Cyber Abilities Worry U.S. Spy Chief.* http://www.reuters.com/article/2011/03/10/us-china-usa-cyber-idUSTRE7295Y820110310 (accessed 12 March 2011).

Richelson, Jeffrey, and Michael Evans. ―Tiananmen Square, 1989: The Declassified History.” http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB16/documents/index.html#f1 (accessed 5 May 2011).

Sharma, Deepak. ―Integrated Network Electronic Warfare: China‘s New Concept of Information Warfare.” *Journal of Defence Studies* 4, no. 2 (April 2010): 38-39. http://www.idsa.in/system/files/jds_4_2_dsharma.pdf (accessed 12 May 2011).

United States Strategic Command. ―Fact Sheets.” http://www.stratcom.mil/factsheets/Cyber_Command/ (accessed 15 January 2011).

Williams, Holly. ―China‘s Cyber Hackers Target Western Firms.” *Skynews*, 18 April 2011. http://news.sky.com/skynews/Home/World-News/Video-Chinas-Cyber-Hackers-Growing-Threat-To-Western-Security-Sky-News-Investigation/Article/201104315974328?lid=ARTICLE_15974328_Video:ChinasCyberHackersGrowingThreatToWesternSecuritySkyNewsInvestigation&lpos=searchresults (accessed 16 May 2011).

The World Bank. http://data.worldbank.org/indicator/NY.GDP.MKTP.CD (accessed 27 April 2011.

Yarger, Harry R. ―Strategic Theory for the 21st Century: The Little Book on Big Strategy.” In C200, *Strategic Environment*, Department of Command and Leadership, 38-44. Fort Leavenworth, KS: Government Printing Office, 2010.

INITIAL DISTRIBUTION LIST

Combined Arms Research Library
U.S. Army Command and General Staff College
250 Gibbon Ave.
Fort Leavenworth, KS 66027-2314

Defense Technical Information Center/OCA
825 John J. Kingman Rd., Suite 944
Fort Belvoir, VA 22060-6218

Mr. Scott A. Porter
Department of Command and Leadership
USACGSC
100 Stimson Ave.
Fort Leavenworth, KS 66027-2301

Dr. David A. Anderson
Department of Interagency, Multi-national, and Joint Operations
USACGSC
100 Stimson Ave.
Fort Leavenworth, KS 66027-2301

Mr. Stephen Melton
Department of Tactics
USACGSC
100 Stimson Ave.
Fort Leavenworth, KS 66027-2301

Mr. Timothy L. Thomas
Foreign Military Studies Office
731 McClellan Ave.
Fort Leavenworth, KS 66027-2301