Three Faces of the CYBER DRAGON

Cyber Peace Activist, Spook, Attacker

和平威慑

侦察战略优势

攻击势

Timothy L. Thomas

Foreign Military Studies Office, Fort Leavenworth, Kansas

Three Faces of the CYBER DRAGON

Cyber Peace Activist, Spook, Attacker

Cover: China's cyber activities are taking three tracks. They are: peaceful intentions (public opinion actions and a military policy of active defense, depicted as the red dragon); espionage (reconnaissance and the stealing of terabytes of information, the white dragon); and preparation for offensive actions (based on mobilization preparations and theoretical writings, the blue dragon).

The author works for the Foreign Military Studies Office (FMSO), Fort Leavenworth, Kansas. FMSO is a component of the US Army's Training and Doctrine Command (TRADOC). The office is charged with preparing studies and assessments based on the reading of foreign and domestic publications and through contacts with a network of foreign and US military and civilian security specialists. FMSO researches, writes, and publishes from unclassified sources about the military establishments, doctrines, and practices of selected foreign armed forces. It also studies a variety of

civilmilitary and transnational security issues affecting the US and its military forces. FMSO products are prepared for the US Army and other services, the Department of Defense, as well as nonDoD organizations to include the Treasury and Justice Departments.

Three Faces of the CYBER DRAGON

Cyber Peace Activist, Spook, Attacker

TIMOTHY L. THOMAS

FOREIGN MILITARY STUDIES OFFICE (FMSO)

FORT LEAVENWORTH, KS

2012

FOREWORD

China's cyber policy has become partly visible to foreign nations through observation, tracking, and inference. The policy appears to have three vectors. The first vector is in the public opinion or "soft power" arena, where China professes to be led by a policy of active defense and cooperation with other nations over cyber issues. The second and most prominent vector is China's exhibited capability to conduct strong and stealthy intelligence and reconnaissance activities against nation's worldwide, using the guise of anonymity to hide these efforts. The third vector is the offensive character of China's cyber strategy. It contains the theoretical backing for preemptive cyber operations against other nations in times of crisis. These three aspects—peace activist, espionage activist, and attack planner—dominate China's cyber policy. Some are always hidden from view while others are demonstrated daily.

Three Faces of the Cyber Dragon is divided into sections that coincide with these vectors. The book first examines soft power theory, information deterrence concepts, and new organizational developments in the People's Liberation Army (PLA) and domestic agencies designed to influence and convince foreign nations of China's peaceful intentions. The work then takes a look at Chinese espionage activities, to include a brief examination of several short case studies on the topic, such as the Aurora, Night Dragon, and Shady Rat incidents. Finally, the PLA's cyber offensive character is examined. There are chapters on China's cyber offensive theory, Blue Army, system sabotage and control theory, system of systems thinking. A final chapter compares Chinese cyber concepts with those in Russia.

China's focus on these three areas of peace activist, espionage activist, and attack planner allow it the flexibility to change and adjust its cyber strategy as needed; and to be ready for future conflicts. The policy appears well grounded in high-level support. *Three Faces of the Cyber Dragon* attempts to provide context to the unfolding nature of China's cyber policy, and gives the analyst a more penetrating look into unconsidered, under-"advertised" aspects of Chinese security thinking.

Thomas Wilhelm
Director, Foreign Military Studies Office
2012

DEDICATION

This book is dedicated to our grandchildren—
Thanks for making your Grandmother and Grandfather's lives brighter!

ACKNOWLEDGEMENT

The author used only open-source translations for the development of this document. Since the author does not speak Chinese, he fully utilized the translation talents of the Open Source Center (formerly the Foreign Broadcast Information Service or FBIS) and other government contracted Chinese translators in order to write this book. The author is solely responsible for the selection and analysis of the material others translated.

Within the Foreign Military Studies Office (FMSO) there are several people to thank. In particular, the author would like to acknowledge the support of Dr. Harold Orenstein of the Foreign Military Studies Office (FMSO). Dr. Orenstein had the difficult task of editing all of the chapters of this book and providing them quickly to speed along the book's printing. His assistance and expertise cannot be underestimated. Without his help the book would not read as clearly as it does. Also due special recognition is Mr. Aaron Perez of FMSO who designed the cover artwork. Mr. Perez's visualization of the contents of this book is well displayed in the images he developed. He is able to take general guidance and turn it into specific, targeted products. Mr. Robert Love of FMSO monitored commercial translations of some material used in this work; Ms. Alice Mink ensured that clearance issues were properly dealt with; D. M. Giangreco is responsible for the final layout of the book; and Mr. Kent Bauman, Deputy Director of FMSO, ensured that funding for the translation of Chinese material was available. Finally, the

author would like to express his thanks to FMSO director Mr. Thomas Wilhelm for providing his support and encouragement of the project.

INTRODUCTION

Because our research is always trailing one step behind countries with highly developed science and technology, we lack strategic innovation and industry-leading momentum. For these reasons, amidst this kind of mutual confrontation, the weaker party can only overcome its opponent by utilizing tactics different from its opponent.[1]

This statement from Fang Binxing, the developer and so-called Father of China's Great Firewall (Internet censor), summarizes the philosophy behind many ongoing Chinese cyber activities. It is increasingly obvious that the Chinese are utilizing tactics different from their opponents, whom they usually claim to be the West. Chinese specialists are often implicated in the theft of digital information from countries across the globe via a combination of digitally inspired traditional and creative oriental methods. These activities have manifested themselves as a three-pronged threat: a cyber soft power threat, a cyber reconnaissance threat, and a cyber attack threat. These threats are referred to here as *The Three Faces of the Cyber Dragon*.

For nearly ten years now Chinese cyber thieves have stolen digital information with impunity. Initially Western analysts could never say for certain where the activities originated or who was involved. Were they watching the work of surrogates, government directed groups, or lone wolf hackers? Recently, however, US analysts have finally been able to ascertain more concretely the precise source of the thievery, as intelligence agencies reportedly have uncovered many of the Chinese groups involved in the cyber spying campaign. According to a recent *Wall Street Journal* report, the People's Liberation Army (PLA) is sponsoring much of the thievery along with some half-dozen nonmilitary groups.[2] The nonmilitary groups are often connected to various organizations, such as universities. James Lewis, a cyber security specialist working at the Center for Strategic and International Studies (who often briefs the Obama administration on such issues), stated that the intelligence work implicating the Chinese involved a combination of cyber forensics and ongoing intelligence collection activities. The Chinese groups are broken down into subgroups based on the type of cyber attack software used, the different Internet addresses employed during the theft, and the manner by which attacks are carried out.[3]

How has China used the information it has reputedly stolen? It is likely that it has reverse engineered many pieces of military equipment, to include (as many analysts suspect) the J-20 stealth bomber, as well as uncovering many of the technical parameters behind the functioning of US equipment. In addition, the Chinese may use the information to construct a modern combat power generation model. One analyst

1 Fang Binxing, in Richard Suttmeier and Xiangkui Yao's report *China's IP Transition*, The National Bureau of Asian Research, Special Report #29, July 2011, p. 22.

2 Siobhan Gorman, "U.S. Homes In on China Spying," The Wall Street Journal, 13 December 2011, p. A11.

3 Ibid.

noted that

> To advance the transformation of combat power generation models into one under informatized conditions, China must energetically develop informatized weapons and equipment, energetically raise the informatization level of the existing weapons and equipment, and advance independent, sustainable weapons and equipment development by leaps and bounds.[4]

To conduct this transformation, information must play the leading role, science and technology are relied upon, and military-civilian integrated development is required.[5] Retired Chinese General Wang Baocun, a noted Chinese information warfare (IW) specialist, stated that as the power of weapons and equipment grows exponentially the combat capabilities of China's forces grow qualitatively. Therefore, the all-inclusive nature of the transformation could also be termed a "quantum leap" in military thinking and modernization in sync with information age developments worldwide and not just a leap-frog endeavor. China's recent development of its Beidou Navigation Satellite System, looked upon by many as an alternative to the US Global Positioning System (GPS), is a case in point. In the past China's military relied on the GPS system and its constellation of 30 satellites. Now China will have its own system and plans to have 16 satellites in orbit by the end of 2012. The Beidou system could be used "in conjunction with other satellites, drones and related technology."[6] The system could track ships or guide antiship ballistic missiles to their targets, or it could help position submarines.[7]

Three Faces of the Cyber Dragon follows the development of Chinese concepts and organizations that are of contemporary concern to the US military. It is important to keep a finger on the pulse of China's military as it proceeds with confidence (and some degree of arrogance) into the second decade of the twenty-first century with an ever expanding cyber force. Following these trends is important for US policy makers as they attempt to make the correct adjustments to US national security policy accordingly. Chapters One through Three discuss soft power advances, Chapters Four through Six discuss reconnaissance activities, and Chapters Seven through Ten discuss offensive cyber activities, the cyber "blue force," and systems of system concepts. It also compares Russian cyber concepts with Chinese concepts. Chapter Eleven highlights the works conclusions.

Chapter One discusses both civilian and military soft power concerns, which elevated in China after leaders witnessed the results of Arab-Spring-type events in the Middle East. China is working to improve its national image abroad, while remaining on guard internally to check the development of similar soft power events in China.

4 Liu Yuejun, "Clearly Understand the Laws Master the Direction Speed-Up Promoting the Change of the Formation Mode of War-Fighting Capabilities," *China Military Science*, No. 3 2011, pp. 87-91, 156.

5 Ibid.

6 Jeremy Page, "Beijing Launches Rival to U.S. GPS System," *The Wall Street Journal*, 28 December 2011, p. A9.

7 Ibid.

The chapter discusses the Chinese belief that the US is trying to divide the Middle Kingdom using ideology and culture. China's external soft power response is to go on a cultural offensive that includes all media assets and even a presence on US soil (Confucius Institutes, CCTV in English [an organization based in Washington, DC], the acquisition of the American Multi-Cinema [AMC] chain, etc.). The goal of China's soft power offensive is to break what its leaders feel is the "verbal hegemony" of the West. Internal civilian soft power issues include the development of an *Internet White Paper* and an international code of conduct on information security. Likewise, China's soft power offensive is felt in the PLA. Soft power is viewed as a strategic resource that uses "intangible swordsmanship, sword spirit, and sword style" to win without fighting. The PLA's external military soft power offensive includes a new focus on the topic of military diplomacy abroad. China's internal PLA soft power offensive includes political officer regulations to control the spread of information; and the development of several websites through which the PLA leadership hopes to seize the initiative in Internet public opinion among servicemen. One PLA author even offers a "how to" for military reporting in the information age.

Chapter Two discusses China's concept of information deterrence and compares it with US concepts. One authoritative PLA book defined information deterrence as having five features: permeability, ambiguity, diversity, two-way containment, and People's War. More importantly, information deterrence creates momentum though military preparation in order to "win victory before the first battle." Power is a key Chinese factor in deterrence theory and thus China must become a cyber power or it will not have deterrent capabilities. Author Cai Cuihong notes that if one nation can control information (attain superiority in this area), then information deterrence can be used to make an adversary lay down his weapons. The PLA's cyber deterrence concept is a combination of ancient/traditional concepts and lessons learned from watching Western nations develop their concepts.

Chapter Three discusses many of the recent developments in China's cyber organization that are designed to enhance deterrence. These include descriptions of new supercomputers and new organizations such as the Strategic Planning Department. Several Chinese concepts have been updated to fit the information age, to include People's War and mobilization contingencies. Newer concepts include a cyber warfare combat model and a network psychological operations organization. The chapter also discusses how China views new US cyber strategies. Overall, US analysts should be concerned about the pace of China's cyber developments as PLA theoreticians attempt to establish the groundwork to achieve a strategic cyber advantage over potential adversaries.

Chapter Four takes a look at the work of US and other Western analysts who are writing about China's cyber concepts and organizations. In spite of continued warnings from the US and several other nations, Chinese cyber theft has continued unabated, an aspect that this chapter also discusses. Some of the reports detailed herein discuss the methods used to infiltrate Western systems, in addition to the wide reach of China's

cyber spooks. Other reports examine China's philosophy behind these efforts. The case studies utilized demonstrate that China's worldwide espionage effort has resulted, at times, in achieving administrative control over some commercial information systems, resulting in the theft of terabytes of information.

Chapter Five discusses in detail the Chinese attack on Google in December and January 2010-2011, code named Operation Aurora. It examines the context within which the Google attacks occurred and how Google's response—challenging Chinese censorship—was used by the Chinese to distract attention from their cyber aggression. It then analyzes how a 2003 military regulation assisted China's response to Google's accusations. The regulation stresses a focus for political officers on the "three warfare" model (media, legal, and psychological warfare). Internal Chinese instructions to newspaper editors regarding how to report the Google affair are included. In short, these procedures are being used all too often by the Chinese and are causing US authorities to be more and more intolerant of Chinese behavior.

Chapter Six discusses the thoughts of several independent writers on the topics of war engineering, war control, and cyber *shi*. All three concepts are foreign to US audiences, although the term "control" is often used in conjunction with the term "command" in US parlance. Two concepts that do appear more Chinese than Western are war engineering and *shi*. War engineering studies, designs, and manages war requirements, theories, experiments, and processes. It has five parts: requirements, planning, testing, control, and evaluation engineering. Control engineering, the most important element, consists of strategic, campaign, and tactical command information systems which monitor situations, control decision making, handle anomalies, and evaluate results.[8] Virtual *shi* involves efforts to attain a strategic advantage in the cyber world. If one is able to do so through planting Trojan horses or viruses or spotting vulnerabilities in Western systems via reconnaissance activities, then it is possible to "win victory before the first battle." That is, planting destructive codes ahead of time via reconnaissance activities that can be activated at a time of China's choosing or knowing a system's weakness ahead of time helps attain the initiative in future battles.

Chapter Seven summarizes the contents of two books and several articles not available when *The Dragon's Quantum Leap*, this author's last book on China, was written in 2009. These summaries include the following elements: several Chinese definitions of information superiority; General (retired) Dai Qingmin's recent writing on integrated network-electronic warfare; and several selected articles on information control and winning local wars under informatized conditions. The heart of these developments lies in the focus on offensive cyber activity and the innovation abilities of the PLA and other institutions. A short discussion of China's initial reaction to the Stuxnet virus (before the *New York Times* claim that the US and Israel were behind the attack) is also included.

Chapter Eight is a look at China's so-called Blue Force, an opposing force (OPFOR) designed to fight in the cyber domain as US cyber forces would fight. It is believed that

8 Ibid.

fighting against a US-type cyber foe will better prepare the PLA in case of a future cyber conflict involving the US. Blue Force successes and the consequences for Red Force commanders who lose cyber encounters are also included in the discussion.

Chapter Nine focuses on the Chinese concept of system of systems (SoS). The PLA focus on SoS operations, discussed somewhat randomly in the past, became an area of devoted and intense scrutiny in 2010-2011. In the first edition of *China Military Science* for 2011, for example, there are seven articles on the SoS topic. They cover laws for developing SoS capabilities; basic SoS issues; technological perspectives of SoS capabilities; building a military forces structure based on the SoS concept; war-fighting capabilities of SoS; SoS and integrated training; and SoS mobilizing capabilities.[9] It is not clear when this discussion period will end, but it is apparent that the PLA is intent on implementing the concept in the shortest possible time frame. It will be well worth the effort to continue to follow the issue in the Chinese press and see where it leads.

Chapter Ten discusses "new concept weapons." These weapons appear to be the next stage for the era beyond cyber or at least an adjunct to it. They include directed-energy weapons, such as lasers, high-powered microwave, particle beam, and sound energy weapons; kinetic energy weapons, such as energy intercept and electromagnetic launch weapons; hypersonic weapons, such as cruise missiles and space combat flight vehicles; and what the Chinese refer to as "nonfatal weapons," such as the space environment, personnel, anti-equipment, and material weapons. Included in the discussion are Chinese research efforts in the areas of rail gun weaponry and electromagnetic pulse weapons.

Chapter Eleven compares recent cyber developments in China with those in Russia. The discussion indicates that there are similarities and differences in the two nations' approaches. China believes that the system of systems concept is the one to follow. China promotes a concept known as integrated network-electronic warfare and focuses on cognitive and technical aspects of cyber along with other issues. Russia is basing much of its cyber efforts on the network-centric concept. Russia still tends to divide its cyber and information warfare effort into information-technical and information-psychological issues. Both countries plan to use cyber deception and electronic warfare means. China tends to focus more on using electrons as stratagems than does Russia, while both nations have a host of excellent algorithm writers.

Chapter Twelve lists the conclusions this analysis has generated, focusing on the three main issues of this text: the three faces of the cyber dragon identified as soft power, reconnaissance, and attack.

The book has two appendixes: one lists information-related articles in the PLA journal *China Military Science* from 2009-2011; and one is a lengthy article on Chinese geostrategic thinking. The purpose of the latter appendix is to offer analysts a paradigm or template into which one can consider how Chinese geopolitical cyber thought might be applied.

This author's prior works on Chinese IW issues include *Dragon Bytes*, which

9 Theme Forum, "Theoretical Research on Systems Operations Based on Information Systems (Part Three), *China Military Science*, No. 1, 2011.

covered Chinese IW activities from 1999-2003; *Decoding the Virtual Dragon*, which covered Chinese IW activities from 2003-2006; and *The Dragon's Quantum Leap*, which covered the period from 2006-2008, with some additional material included from earlier years. These three works, as well as this current book, serve as a guide to understanding the PLA's information-based transformation efforts. Hopefully these books provide a progressive look at Chinese cyber issues and assist analysts in visualizing the broader context from which Chinese cyber issues are emerging. The added hope is that the works enable analysts to draw a more realistic picture of the challenge the PLA presents in the IW arena, as well as a perspective for choosing potential future areas of collaboration.

PART ONE
CYBER PEACE ACTIVIST

CHAPTER ONE
CHINA'S INTERNAL AND EXTERNAL SOFT POWER OFFENSIVE

Hard power is a race for military, economic, and technological power. Hard power wars are about the occupation of land, but soft power battles are about seizing space in information, stories, ideas, and ideology.[10]

Introduction

The principal vector China uses to advance its cyber peace activist agenda is through a soft power offense. The offensive has internal and external civilian and military aspects and carries top level support. At the beginning of 2012, Chinese President Hu Jintao called upon the Communist Party of China (CPC) to fight against international forces that, in his opinion, are trying to divide China using ideology and culture. "We must be aware of the seriousness and complexity of the struggles and take powerful measures to prevent and deal with them," he warned in an article in the Communist Party magazine *Qiushi*.[11]

The Party has taken a number of steps to fulfill his wish. Internally, China's civilian and military propaganda apparatus is trying to compete with Chinese Internet search engines and social networking sites like Sina, Sohu, and Baidu for public influence. Externally, the Party has been much more aggressive with public and military effort to influence foreign media, primarily directed against the US. For example, the official state-run news agency *Xinhua* is promoting itself on a giant electronic billboard in Times Square. China's Central Television, CCTV, is leasing space in Manhattan and building a United States broadcasting center in Washington.[12] It is hoped, according to another report, that the DC office will compete with CNN, the BBC, and al-Jazeera. China's ambition is to "use news reporting and cultural programming to advance its 'soft power' or cultural influence."[13] The *China Daily* has taken out "China Watch" center page ads in the *New York Times* and *Wall Street Journal* that focus on the culture and achievements of the Chinese nation. In 2010 the Party advanced an *Internet White Paper* and in 2011 a code of conduct for information security at the United Nation.

The People's Liberation Army (PLA) is part of the internal and external soft power

---

10 Li Xiguang, "Soft Power's Reach Depends on Friendly Internet," *Global Times* Online, 2 November 2010.

11 Peter Simpson, "Chinese President Hu Jintao Warns of Cultural Warfare from the West," *The Telegraph*, 2 January 2012, downloaded from http://www.telegraph.co.uk/news/worldnews/asia/china/8988195/Chinese-President-Hu-Jintao-warns-of-cultural-warfare-from-West.html#disqus_thread.

12 David Barboza, "Unit of Chinese Daily Plans I.P.O.," *The New York Times International*, Sunday 15 January 2012, p. 8.

13 Paul Farhi, "In D.C., China Builds a News Hub to Help Polish its Global Image," http://www.washingtonpost.com/paul-farhi/2011/03/08/ABO2YCP_page.html.

effort as well. A report in the official publication of the military's Academy of Military Science, *China Military Science*, noted that China must take action "to propel China's culture industry and media industry beyond China's borders in an effort to take over the international culture market."[14] In short, there is an all-out soft power assault underway, both internally and externally, under the direction of the CPC.

This chapter first will discuss the comments and projects of civilians as they develop China's soft power capability. The chapter then shifts to the military directives on soft power use in the military media and in military diplomacy. The chapter ends with the PLA's "three warfares" (public opinion warfare, psychological warfare, and legal warfare) concept found in the political work regulation.

Background

China has achieved a remarkable growth in its hard power military force. There has been considerable progress and technological advancements in the construction of tanks, missiles, planes, and ships. These elements are easy to spot and their characteristics and effects are easy to describe. The elements of soft power, which have not experienced the same growth, are harder to recognize, but progress is underway there as well. Soft power is, from the Chinese perspective, thought to include media, public opinion, psychological, and legal issues.

A growing realization in China today is that soft power is nearly as meaningful as hard power for two reasons. First, high-tech media applications (TaoTao or the Twitter equivalent, Yupoo or the Flickr equivalent, Tudou.com or the YouTube equivalent, etc.) have become reliable ways to influence groups of people in ways not imaginable in the past. Second, soft power is vitally important when viewed from the Chinese context of fostering the ability to "win without fighting." How China can become a legitimate "soft power" power has thus become a question of extreme importance to its leaders. Further, China must master soft power if it is to prevent a repetition of events that took place in Tunisia, Libya, and Egypt. In February 2011 China did successfully thwart a mini-uprising known as the Jasmine revolution, which was an attempt at an Arab-Spring-type event.[15] The Jasmine revolution was an online movement that attempted to gain momentum from the fomenting revolutions that started in Tunisia in December 2010. However, the CPC was able to exert its own form of cyber control over the movement through passive measures such as extensive information monitoring and information blocking initiatives; and through active measures that included information attacks, intimidation, campaigning, and self-censorship. Both cases involved the blockage of words, phrases, and topics considered off limits.[16]

To increase its civilian soft power potential, China is focusing on growing its media

14 Wang Shudao, "Modern Cultural Diffusion and National Security," *China Military Science*, No. 3 2005, pp. 64-69.

15 For an excellent explanation of the Jasmine Revolution, see Scott Henderson, "Whither the Jasmine Revolution: China's Two Phase Operation for In-Depth Cyber Control," forthcoming in *Air Power Journal*, 2012.

16 Ibid. Mr. Henderson works for the Foreign Military Studies Office and provided the author access to his article.

and public diplomacy capabilities. Li Changchun, a member of the standing committee of the CPC's Central Committee Political Bureau, stated in March 2011 that China must boost the integration of telecommunications networks, cable TV networks, and the Internet in order to promote the competitiveness of China's culture[17] and thus its national image and soft power. The nation must be capable of using both traditional media and new media to influence people and convince them of China's peaceful and diplomatic path of development.

China's biggest soft power vulnerability is thought to be the Internet. In the information age China's analysts understand that the Internet offers many opportunities for influence activities to be fostered and developed in other countries. Information technology has also opened the door for creative thought in the area of digital deception. Such activities can include the manipulation of public opinion and the potential creation of divisions within a society by actually goading groups into action.

Some Chinese scholars envy US thinking on strategic communications and influence activities. For example, a 2010 *Global Times* commentary by Li Xiguang, a professor at Tsinghua University in China, noted that "China should learn from the US in planning a global strategic communication system and building a global social network through which to nurture pro-Chinese scholars." [18]

The focus on improving China's soft power and public diplomacy capabilities has carried over to the military. The PLA has written extensively on the methods and principles involved in raising China's external military diplomacy and improving its internal soft power capabilities to improve the will power of its soldiers. The PLA's Nanjing Institute of Politics appears to play a key role in this effort. The PLA recognizes that the social context for soldiers has changed, as each serviceman can access alternate sources of information. This requires "counter" input to foreign or domestic soft power that works against Chinese patriotism. The overall purpose is to strengthen a soldier's morale.

A soldier's context must be "cleaned of noise" that is damaging to military culture and the army's soul. It is important to properly manage the construction of the Internet to enable political officers to attain their goal of improving the will power of soldiers. The PLA must become skilled at "using micro-blogs, forums, blogs, cell phones, and other such platforms, adopting animated cartoons, videos, pictures, poems, and songs" in order to guide public opinion in both non-war and wartime situations.[19] The threats are numerous. One article included "non-party affiliation, de-politicization, and nationalization of the army"[20] as potential threats to the army's soul.

The end goal of the using strategic influence weapons is to change the balance of soft power in China's favor. Many challenges remain to maintain ideological security,

17 *Xinhua News Agency*, 24 March 2011.

18 Ibid.

19 Zhang Jianhua, "Non-War Military Actions and the Role of the New Media," *Jiefangjun Bao* Online, 11 October 2011, p. 7.

20 Staff Commentator, "Building New Platform, Fostering New Skills—Fourth Commentary on Profoundly and Persistently Cultivating Core Values of Contemporary Revolutionary Servicemen," *Jiefangjun Bao* Online, 7 June 2011, p. 1.

uphold unit solidarity, carry out diversified mission tasking, and improve China's national image. To win with soft power, China's leaders must react to situations with speed and seize the initiative. Responses to negative information must be positive and prudent and faced squarely. Finally, rules must be followed.

Civilian Issues: China's Public Diplomacy/National Image Concepts

There are several ways that China has influenced its soft power offensive both internally and externally in the civilian sphere. Four that stand out are the state's United Nations code of conduct proposal on information security, *Internet White Paper*, public diplomacy developments, and efforts at image-building. All four are tightly integrated and represent the avenues through which China hopes to influence its own citizens and decision-makers, as well as citizens abroad.

United Nations Code of Conduct Proposal

China, Russia, Tajikistan, and Uzbekistan sent a letter to the Secretary-General of the United Nations, dated 12 September 2011, calling for "international deliberations within the United Nations framework"[21] on an international code of conduct for information security. The stated goal of these countries is to "prevent the potential use of information and communication technologies for purposes that are inconsistent with the objectives of maintaining international stability and security."[22] Of equal concern was that these information technologies could "adversely affect the integrity of the infrastructure within States."[23]

The UN letter was signed by Li Baodong, Permanent Representative of the People's Republic of China to the United Nations, and distributed on 14 September 2011. Key elements in the code appear to be the following:

> Reaffirming that policy authority for Internet-related public issues is the sovereign right of States, which have rights and responsibilities for international Internet-related public policy issues…[24]

> Each state voluntarily subscribing to the code pledges to comply with the Charter of the UN and universally recognized norms governing international relations that enshrine, *inter alia*, respect for the sovereignty, territorial integrity, and political independence of all States…[25]

In addition to issues of sovereignty, other areas of concern to these four countries appear to be any cyber issue that threatens the "political, economic, and social security

21 "Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan, and Uzbekistan to the United Nations Addressed to the Secretary-General," Sixty-sixth Session of the United Nations General Assembly, dated 14 September 2011, p. 1.

22 Ibid., p. 3.

23 Ibid.

24 Ibid.

25 Ibid., p. 4.

of other countries."[26] States are to curb the "dissemination of information that incites terrorism, secessionism, or extremism or that undermines other countries' political, economic, and social stability, as well as their spiritual and cultural environment."[27]

Several Chinese analysts commented on the code of conduct. Shen Yi, from Fudan University's School of International Studies and Public Affairs, stated that the code of conduct hopes to "reach a consensus on international norms and rules"[28] to regulate the cyber conduct of all countries. The goal is to help underdeveloped countries weak in information technologies from being placed in a disadvantageous position for information dissemination. The idea is to emphasize sovereign equality. Shen contrasts this approach with the European and US positions, which in his opinion only seek to expand their own national interests with the help of technological and media outlets.[29]

Zhang Zhe, a staff reporter for *Dongfang Zaobao* Online, offered a similar appraisal of the code of conduct from a Chinese perspective. He noted that the emphasis of the code on sovereignty reflects Chinese characteristics and that the decision-making power on any Internet-related public policy issue is the sovereign right of the countries in question. China believes that the flow of information should not be used to compromise a state's sovereignty.[30] The code also "has specifically set a relevant provision to limit US military operations."[31] The US wants cooperation among governments and between governments and companies, while China's approach is based on agreement among the international community.[32]

Some Western analysts strongly disagreed with the code of conduct concept. Martin Mueller, a Syracuse University professor and Internet governance expert, feels a code of conduct will attempt to "overlay territorial sovereignty on an Internet that is fundamentally inconsistent with it."[33] Analyst Nate Anderson feels the code aims to stake out territory for nation-states on the Internet. He adds that "it is not hard to see how curbing information that undermines 'social stability' is going to lead to problems; indeed, the generality of the wording is part of the problem."[34]

Internet White Paper

China's *2010 Internet White Paper* stresses the scientific development, active use, law-based administration, and security of the Internet. If these principles are followed, the paper adds, it is believed that social harmony and economic prosperity will follow and science and technology will be advanced.

---

26 Ibid.

27 Ibid.

28 Shen Yi, "Weak Nations' 'Right to Speak' in Cyberspace Should Not Be Deprived," *Wen Hui Bao* Online, 14 September 2011.

29 Ibid.

30 Zhang Zhe, "China and Russia Spearhead the Promotion of a Cyberspace Code of Conduct to Counter the United States," *Dongfang Zaobao* Online, 14 September 2011.

31 Ibid.

32 Ibid.

33 Nate Anderson, "Russia, China, Tajikistan Propose UN 'Code of Conduct' for the Net," downloaded at http://arstechnica.com/tech-policy/news/2011/09.

34 Ibid.

The paper states that in 2010 China's State Council decided to accelerate the integration of radio, TV, and the Internet in order to further develop the information and culture industries. The *White Paper* notes, for example, that China is attempting to spread its culture via the Internet, having established over 300,000 online data bases; and that "cyber culture has become an important component of the Chinese culture industry."[35]

Some of the interesting statistics from the *White Paper* include the following:

- From 1997 to 2009 4.3 trillion Yuan were spent on Internet infrastructure construction, including the building of an 8.267-million-km optical communication network;
- At the end of 2009, there were 136 million broadband Internet access ports;
- International outlet bandwidth was 866,367 Gbps, with seven land-submarine cables and twenty land cables, ensuring Inter-net access to 99.3% of Chinese towns and 91.5% of villages;
- By the end of 2009 there were 384 million "netizens" with an annual increase of 31.95 million users;
- There were 3.23 million websites in 2009, 2,152 times that of 1997;
- Broadband use reached 346 million people while 233 million people used mobile phones to access the Internet
- Urban Internet use made up 72.2% of the national total;
- In 2009 46 million people received an education with Internet help, 35 million conducted securities trading on the Internet, 15 million sought jobs through the Internet, and 14 million arranged trips via the Internet;
- Online gaming produced 25.8 billion Yuan in 2009, a 39.5% increase over 2008;
- Over 80% of county-level governments had set up websites and reportedly 80% of China's netizens rely on the Internet for news. The Internet became a method to obtain news from sites such as People's Daily Online, Xinhuanet, CCTV.com, and CNR.cn.[36]

The government is aware that social conditions and public opinion are items to be closely monitored on the Internet. Internet use must be rational [the latter being a term defined by the authorities!], which includes the use of technical means that "prevent and curb the harmful effects of illegal information on state security, public interests, and minors."[37] Further, no individual or organization may "jeopardize state security, the public interest, or the legitimate rights and interests of other people."[38]

The state founded the Internet Society of China (ISC) to promote self-regulation

35 "The Internet in China," *Xinhua* (in English), 8 June 2010.
36 Ibid.
37 Ibid.
38 Ibid.

and public supervision of the Internet. The ISC not only has worked to reduce spam, but has also produced a list of self-disciplinary regulations that include a number of public pledges. The *White Paper* states that "Chinese laws prohibit all forms of hacking," a statement viewed with skepticism by a growing number of nation-states that have been attacked by Chinese hackers. These nations would question the Chinese authorities' interest in implementing such a law. Finally, the *White Paper* notes that China believes the "United Nations should be given full scope in international Internet administration" and that all countries need multilevel exchanges and cooperation on the basis of equality and mutual benefit.[39]

Public Diplomacy

Zhang Zhexin of China's Shanghai Institute for International Studies (ISS), speaking at a US InfoWarCon conference in 2009, defined public diplomacy (PD) and provided a short history of the concepts development in China. PD is defined as "the process by which direct exchanges and communications with people in a country are conducted to advance the image and extend the values of those being represented."[40] A PD institute is defined as "the organization of public diplomacy-related agencies, their separate responsibilities, and means of public diplomacy practice."[41] Zhang stated that PD is comprised of the short-term goal-oriented "international information communications (IIC)" and the long-term objective "international cultural communications (ICC)."[42]

Zhang listed three phases of China's PD development. First was the period from 1949 to the late 1980s, a period marked by the glorification of China abroad in foreign propaganda and the exertion of control over domestic information. The founding of international newspapers occurred. The second phase started at the end of the Cold War and continued until the beginning of the 21st century. This phase included a move away from one-way foreign propaganda to two-way international communications, where China was publicized but not glorified. A national Internet broadcast system was developed, to include the *People's Daily* Online and *Xinhua News* Online. The image of China in foreign media as an emerging threat appeared in phase two. The third phase started around 2003, but Zhang offered no end point. This phase offered PD theory-building, more focus on ICC (such as the establishment of a few hundred Confucius Institutes worldwide, which extol the virtues of Chinese culture), and platforms for the Internet and mobile phones.[43]

On 11 September 2010 a Center for Public Diplomacy was established in China at Beijing's Foreign Studies University. The goal of such an enterprise was to integrate and coordinate China's ICC and IIC efforts. As a result of this development, forums have been held to help improve China's PD efforts. The university has served two purposes. First, its establishment has offered a way for China's PD effort to confront or adjust to

39 Ibid.

40 Zhang Zhexin, "China's Public Diplomacy Institution: Its Development, Challenges, and Prospects of Its Practice," *IO Journal*, December 2009, p. 13.

41 Ibid.

42 Ibid.

43 Ibid.

the continually changing international and technological environment. Second, China hopes to use the Center to better explain its overall goals and intentions to alleviate the alarm and trumpeting of China threat theories in the international community caused by China's growing economic potential and overall rise in strength. In addition to the Center for Public Diplomacy, numerous other means have been used to alleviate concern, such as the recent media publication of a 2011 White Paper on China's Peaceful Development. Overall these means have gained traction, more so in underdeveloped nations than in developed ones.

However, Fu Ying, a Vice Foreign Minister responsible for PD, stated that China is still far from having a PD system like that of other countries. China's image in the foreign press, she added, depends on the country presenting itself more completely.[44] In 2009 Zhang had stated that the goal of China was "not to challenge or even impair other countries' images but to create a confident, open, and responsible image for itself, represented in the vision of a 'harmonious world.'"[45]

National Image

Insights into China's goals and intentions can be gained through an understanding of the nation's concept of "national image." China is not just calligraphy, the opera, acrobatics, Peking roast duck, and the Great Wall. The projection of national image comes from a country's values, political system, and domestic and foreign policies. These elements influence the generation of a particular type of soft power with Chinese characteristics. The core element of soft power is its ability to unify a nation and a society due to these policies. China recognizes that today soft power is strongly influenced by the interpretation of Internet-based information in a network-centered society. [46]

Chinese professor Li Geqin has defined national image as a "comparatively stable general appraisal of a country by the international community, or the accumulation of general impressions on a country spread via international media by this country in the international community."[47] Further, national image refers to the basic spiritual appearance and political reputation of a country in the international community. It includes the self-image of a country and others impressions of that country. Some even consider national image to be a country's strategic resource.[48]

Li notes that China, when defining national image, works to create and display an image of a strong government, a united Chinese nation, an ancient culture, a harmonious society, and an affluent people with a friendliness and responsibility to foreign countries. At the moment the focus appears to be on ancient culture and the Chinese language in the ads the Chinese have placed in US newspapers. Western societies, Li notes, believe that national image is characterized by democratic elections,

44 Wu Jiao and Ai Yang, "Putting China's Best Face Forward," *China Daily* Online (in English), 12 September 2010.

45 Zhang Zhexin, p. 17.

46 Li Xiguang.

47 Li Geqin, "Growth of a Power and the Shaping of China's National Image," *Xiandai Guoji Guanxi*, 20 October 2008, pp. 40-46.

48 Ibid.

limited government, a humanitarian and rule-of-law society, a general public that enjoys freedom and human rights, and minority ethnic rights.[49]

To create China's national image as a world power, Li writes that China must develop an all-round strategy that is capable of influencing and convincing foreign media and citizens of China's peaceful intentions. The strategy includes the following points. First, China must narrow the Sino-Western political and cultural gaps and create common room for dialogue. China's transmission of information must agree with mainstream international political, cultural, and value systems as much as possible. China has recognized the norms and values of peaceful opposition to violence and the need for compliance with acts of humanitarianism, ecological and environmental protection, civil society, and a government of honesty. This has required transcending ideological and cultural barriers.[50]

Second, China should cultivate diverse participation in activities, reduce direct government footprints, and increase nongovernmental Chinese organizational input. Third, national image depends on speaking as well as doing. In addition to providing peacekeepers, China must advocate international agendas and agreements regarding basic norms and values for security, environmental protection, and other important global issues.[51]

Fourth, international relations require a value-oriented foundation. The Chinese government has attempted to motivate this type of thought and actions through the concept of a harmonious world as a way to spread common values. Finally, China must be rational about censures and prejudices against it or praise for it. China should be confident and optimistic, but also be willing to accept criticism and not react in an irrational patriotic and extreme nationalist manner.[52] It is clear, based on the actions of the Chinese state, that Li is speaking for himself and not for the collective whole of government with regard to many of his recommendations.

Zhang Zuorong, the Deputy Director of the Propaganda Department of Hainan's CPC Committee, noted in 2011 that in order to construct a national image, China needs a timetable and roadmap; a scientifically determined time, order, and progress of events; defined responsibilities; and progress in an efficient and orderly manner. Trust must be increased and anxieties dispelled. Further, the psychological features, habits, and interests of foreign audiences must be studied to find out what they need and in what form, that is, know their likes and dislikes. China must convert the advantages of the modern media into competitive advantages. To this end, China must "establish a number of internationally influential modern media groups that provide multi-language services that have a large audience, that provide sufficient information, that have credibility, and that have discourse power."[53] The current advertising onslaught directed at US media appears to be the start of such a campaign.

49 Ibid.

50 Ibid.

51 Ibid.

52 Ibid.

53 Zhang Zuorong, "Apply Modern Media to Strengthen Building of National Image," *Renmin Ribao* Online, 10 March 2011, p. 21.

Yu Jianrong, director of the Institute of Rural Development at the Chinese Academy of Social Sciences, stated that in 2010 that China's image was one of contradiction. The cultivated image of a country capable of hosting huge international gatherings (Olympics, Shanghai Expo, etc.) was still associated with the more traditional consumer goods and travel terms "made in China" or the Great Wall. That is, there was an under appreciation for all that China was doing. Therefore, on October 1 the State Council Information Office shot a publicity film that included celebrities such as China's first astronaut, Yang Liwei, and NBA basketball star Yao Ming. China, however, has been its own worst enemy at times in the media market. For example, the country's refusal to criticize North Korea for its shelling and killing of four South Koreans stands out.[54] This indicates that the construction of China's national image is either a work in progress or a work that has specific bounds it will not exceed, such as criticizing a close ally.

One of the primary tools used to shape China's national image is the *Xinhua News Agency*. The agency shapes China's image both at home and abroad. Literally "New China News Agency," this organization is the largest press agency of the government of the People's Republic of China (PRC) and its official one. *Xinhua* is subordinate to the PRC State Council and reports to the CPC's Publicity and Public Information Department.[55] Therefore its domestic responsibilities are at the apex of the organization's charter. However, *Xinhua* has an international role to play. It hopes to "break the monopoly and verbal hegemony" of the West. In recent months it has signed agreements with Cuba, Mongolia, Malaysia, Vietnam, Turkey, Nigeria, and Zimbabwe, making it a leading source of news for parts of Asia and Africa. Today there is even an iPhone app for "*Xinhua* news, cartoons, financial information."[56]

Internationally, China has spread the development of Confucius Institutes around the globe. As of July 2010 there were 316 such institutes and 337 classrooms in 94 countries and regions. The US has 57 such institutes at universities. The Office of the Chinese Language Council International (Hanban) aims to establish 1000 Confucius Institutes by 2020.[57]

Internal Soft Power Battles

Not all is running smoothly in China's soft power regime, however. China is experiencing internal friction among its information technology elite. A recent software battle between Tencent and Qihoo, two very successful software companies, underscores this point. Tencent's empire is built on QQ, an instant messaging service. Qihoo owns the second most popular software download in China, 360, a free antivirus program. The dispute apparently began when Tencent promoted a free security download, QQ Doctor. This infringed on the sales of 360. Qihoo responded with a program called "Koukou Bodyguard," which sounds similar to QQ in Chinese. Koukou Bodyguard

54 Lin Meilian, "Selling the Friendly Dragon," *Global Times* Online (in English), 20 December 2010.

55 *Xinhua News Agency*, *Wikipedia*, at https://en.wikipedia.org/wiki/Xinhua

56 Isaac Stone Fish, "All the Propaganda That's Fit to Print," located at http://www.thedaily beast.com/newsweek/2010/09/03/is-china-s-xinhua-the-future-of-journ…

57 Confucius Institute, *Wikipedia*, at http://en.wikipedia.org/wiki/Confucius_Institute

targeted Tencent's instant messaging service with a new program that allowed users to disable plug-ins and advertisements on QQ's site, areas from which Tencent drew almost half of its revenue.[58] Such internal battles for income are expected to continue into the next decade.

Military Issues: Military Soft Power and Military Diplomacy

Zeng Jia, an associate professor in the Department of Military News Dissemination at the PLA's Nanjing Institute of Politics, wrote that the PLA is involved in putting together a diplomatic offensive to increase its soft power potential in what it terms the "omnipresent network age."[59] The goal of this offensive could be, as Wang Shudao notes above, to "take over the international culture market."

Military Soft Power

Wang Xingsheng and Wu Zhizhong, writing in 2007 in the journal *China Military Science*, referred to soft power as a strategic resource that all nations must possess. Soft power consists of intangible elements (culture, theory, tradition, sprit, image, etc.) that integrate with other means and weapons to create an effective fighting force. Soft power unifies officers and soldiers and the military and civilians of a nation. The military's image is the core element of soft military power. It influences how tasks are completed and the realization of political objectives. Safeguarding China's national and military images are important strategic tasks. A military news team, Wang and Wu suggest, should be established to uphold the army's image.[60] Further, the strategies and tactics designed to safeguard national interests must uphold international justice.

Yang Chunchang, a deputy head of the Military Construction Department of China's Academy of Military Science, defined military soft power three years later as the ability to penetrate and constrain people's thinking and cognitive processes. It can mobilize power and exploit military qualities such as culture and diplomacy. It can also deter and destroy an enemy force or influence friends. Further, military soft power has the ability to penetrate and constrain people's thinking and mentality. It uses intangible swordsmanship, sword spirit, and sword style, not the sharp sword, to win without fighting. It commands respect with virtue, benevolence, and generous support.[61]

The journal *China Military Science* has continued to publish articles on soft power. For example, in 2011 Xiao Jingmin, a technical specialist and researcher in the Department of War Theory and Strategic Studies at the PLA's Academy of Military Science, stated that soft power is a type of resolute, flexible, and dynamic mental power required to influence and solidify strategic will, wisdom, and plans to defend national security and developmental interests. It is an extension and deepening of the concept of

58 Yu Xiaodong, "Choosing Sides," NEWSCHINA, January 2011, p. 31.

59 Zeng Jia, "Omnipresent External Dissemination of Military News, *Junshi Jizhe*, 15-16 March, 2011, pp. 53-54.

60 Wang Xingsheng and Wu Zhizhong, "On Building Soft Military Power," *China Military Science*, No. 1 2007, pp. 92-98.

61 Yang Chunchang, "Building Military Soft Power," *Renmin Ribao* Online, 19 May 2010, p. 23.

national soft power in the political science field, and is an aspect of the comprehensive national power system. More formally, Xiao defines soft power in the following manner:

> Soft power of national defense mainly refers to the collective of a country's national defensive will, anti-aggression tradition, strategic thinking, and national defense culture and ideas, that it is a tenacious, invisible, and flexible power, a power than can strengthen the national defensive will and the spirit of a state, nation, or society, an inherent, everlasting support power throughout the ages for maintaining national security and realizing national development.[62]

Soft power serves as a deterrent power due to its ability to mobilize the nation to resist foreign invasions and to serve as a supporting asset for the People's War concept. It thereby causes adversaries to think twice before attacking.[63]

Soft power of national defense includes the army's political will, military theories, traditional style, use of stratagems, and structure and mechanisms. At the strategic level, the party leadership is able to respond to threats and challenges with strategic will, strategic wisdom, and strategic operations research. Hard power, on the other hand, remains the objective basis for the use of soft power, the latter being composed of subjective spiritual elements. Without hard power elements such as economic and science and technological developments, soft power won't work. Together they produce effects and influence.[64]

Three authors from the Nanjing Army Command Academy offered one final soft power definition in *China Military Science* in 2011. They defined the term as "a country's and military's ability to influence and mold others through nonphysical forces such as military culture, military spirit, military image, and military diplomacy in military affairs practices, thereby achieving the objectives of their military strategy."[65]

Some PLA members have respect bordering on fear for the influence of soft power. For example, National Defense University Professor Han Xudong considers soft power a new type of global warfare initiated by the United States. He notes that network space, the foundation for society's existence and development today, will be the primary battlefield of future war. The only world power with access to this space and with the ability to launch soft-power gamesmanship is the US. Network space enables the US to occupy public opinion's high ground; to generate deterrence through the use of advanced technology; and to strive for total dominance, since it can establish the rules of the game. China must work hard to understand the new features of this new form of warfare, in Han's opinion.[66] Two months later, Han called for the establishment of

62 Xiao Jingmin, "Theoretical Exploration of Soft Power in China's National Defense," *China Military Science*, No. 3 2011, pp. 131-138.

63 Ibid.

64 Ibid.

65 Tian Xiang, Chen Yongqiang, and Ding Jun, "An Analysis of the PLA's Image—Building from the Perspective of Military Soft Power," *China Military Science*, No. 4 2010, pp. 116-124.

66 Han Xudong, "A New Form of Global Warfare by the United States," *Liaowang*, No. 40-41 10

cyber armament controls, again citing the advancements of the US in the cyber arena. Missing from his entire analysis was any mention of what the PLA was doing in this arena, and they are doing a lot. As a result Western analysts tend to ignore Han's one-sided discourse on the need for cyber arms control.

Elements of China's soft power approach appear to include military diplomacy and the "three warfares (public opinion [media] warfare, psychological warfare, law warfare)." These elements, along with China's new-found media confidence and the limits placed on a PLA soldier's Internet use, are discussed next in greater detail.

Military Diplomacy

Qian Lihua, the Director-General of the Foreign Affairs Office of the Ministry of National Defense of China, defined military diplomacy as "a strategic means of safeguarding national sovereignty, security and developmental interests, and the in-depth reflection of the strategic mutual-trust and cooperative level between Chinese and foreign parties."[67] Military diplomacy thus creates an external environment conducive for China's development.

The military diplomacy concept was advanced further in a 6 February 2011 *Guangming Ribao* Online report. Author Zhu Chenghu, the Director of a Strategic Research and Teaching Office at National Defense University, stated that promoting military diplomacy is a contemporary topic where dangers intertwine with opportunities. Zhu stated that military diplomacy is infiltrating military cooperation and extending the enhancement of regional security cooperation. Military diplomacy will "strive to use military cooperation to increase the achievements of peaceful diplomacy, expand the influence of peaceful diplomacy, and attract as many people as possible to jointly promote peace."[68]

Military diplomacy is political competition in the military sphere, according to Zhu. This requires that China study, master, and use law to support military diplomacy to win a bigger say in international military affairs and better defend China's national interests. "Strategies should be combined with legal war to better handle territorial and maritime territorial conflicts and clashes, to include those to come in outer space."[69]

On 1 August 2011 the MOD's official website, which is www.mod. gov.cn, went into full operation. It had been run on a trial basis for two years.[70] The development of an MOD website supports the fact that China needs to upgrade its traditional national defense concept since, according to one source, the future center of gravity will be cultural national defense. A specialized cultural national defense force, armed with scientists, information experts, and servicemen who are proficient in information

October 2011, p. 96.

67 Zhou Feng, "Interview: Splendor of China's Military Diplomacy in the Last Five Years," *Jiefangjun Bao* Online, 30 November 2010.

68 Zhu Chenghu, "We Possess It Because We Stopped War—Analysis of the Peaceful Duties of China's Military Diplomacy," Beijing *Guangming Ribao* Online, 6 February 2011.

69 Ibid.

70 Unattributed article, "China to Boost Military Development under New Model/Politics," *China Daily* Online (in English), 2 August 2011.

warfare, needs to be created. Their main task will be to defend the information frontiers of China, counter the information aggressiveness of other nations, and prevent cyber incidents from occurring.[71]

Much like their civilian counterparts, China's military is focused on increasing its public and military diplomatic posture, as well as its military's image-making capability. The Ministry of Defense (MOD) website has developed a free Android operating system platform-based terminal. While tailored to Android users, there is an interface consistent with the MOD's iPhone terminal. It contains nine columns of news on the armed forces, military situations, photos and videos, and other military information for public image consumption.

An MOD mobile phone website (wap.mod.gov.cn) was also tested. This website and the MOD official website are designed to communicate China's national defense prowess to the world and display the proper image of China's armed forces. The site seeks to guide public opinion, reporter Zheng Wenda noted, through its authoritativeness and service orientation.[72]

The theme of military diplomacy's smokeless battlefield is to remove external obstacles for China's military modernization. The goal is to remove the China military threat theory from any soil. In the end this will enable foreign countries to participate in the military modernization of China once these theories are eliminated.[73] In examining Chinese theories of legal warfare, China tends to look at law differently than does the US. Some worry that Western interpretations of law actually assist the Chi-nese, while the Chinese selectively choose what information to release or discuss.

Image-making, a key aspect of China's civilian approach to soft power, is also a key part of China's military diplomacy. A September 2010 seminar at Nanjing's Institute of Politics centered on five topics associated with image-making: the strategy of image-portrayal of the PLA; basic paths and ways to portray the PLA's international image; the strategy for spreading the military's image; the basic experiences and innovations for portraying the PLA's international image; and foreign military image building and its background.[74]

Military attaches have been given a role in spreading China's culture. A *Jiefangjun Bao* headline recently noted that "Chinese Military Attachés Actively Introduce China to Outside World."[75] Li Jun, identified as China's military attaché to Serbia, noted that China, faced with media attacks that distort China's development strategy and magnify its military power, "must utter our own voice, otherwise foreign people will form biases

---

71 Yue Housheng, "New Thinking on Cultural Military Strategy," *Jiefangjun Bao* Online, 1 February 2011, p. 7.

72 Zheng Wenda, "Disseminate Information about China's National Defense Policies, Project the Image of the Chinese Army," *Jiefangjun Bao* Online, 2 August 2011, p. 9.

73 Zhu.

74 Wang Wei and Zhang Feng, "Theoretical Seminar on the PLA's Foreign Publicity Work Held," Ministry of National Defense of the People's Republic of China (in English) website, http://eng.mod.gov.cn, 10 September 2010.

75 Chang Qianjin, Zhong Yang, and Luo Zheng, "Chinese Military Attaches Actively Introduce China to the Outside World," *Jiefangjun Bao* Online (in English), 3 September 2010.

about China since what they hear and see is one-sided in that regard."[76]

The military diplomacy concept has seemingly continued to develop. In early 2012 the term was defined in the following manner:

> Military diplomacy refers to external military exchanges with armed forces as the main body. External propaganda of military affairs is the indispensable "business card" during external military exchanges. It undertakes the task of creating the image of the main body for military diplomacy…Through multiple means an all-directional, multi-layer, and wide-range external military exchange pattern has been formed.[77]

Author Zhang Fang goes on to note that the multiple means he mentions include contacts between military leaders and professional technicians, exchange visits between military vessels and recreation and sports exchanges, and the "fulfillment of promises about arms control, military technology cooperation with foreign countries, personnel training, importing intelligence, and participating in the peacekeeping mission of the United Nations."[78] Further, Zhang points out the requirement to look for successful penetration points in foreign media and to master the social awareness and means of influencing target populations. This includes mastering the strategic application of language to accomplish national security goals, such as using the term Ryukyu Islands instead of Okinawa when discussing Japanese issues. Tracking the influence of foreign propaganda on international opinion is also necessary in order to attain the proper and correct feedback.[79]

Military Media in the International Environment

China's analysts understand that the public opinion environment can help or restrict the development of a nation's military. The PLA wants to use public opinion and the international media to its advantage. Meng Yan, writing in 2011, stated that Western media currently have the power to define the image of China (and other countries!), and China must work to counter this tendency.[80]

Meng notes that "the image of a military is made up of the components of its objective image, public image, and media image."[81] Objective images exist in reality, public images depend on contacts and awareness, and media images depend on subjective impressions created by descriptions. The PLA feels it has been more transparent and open than at any time in the recent past, yet people are only utilizing this openness to say China is a threat. Regardless, Meng adds, the PLA knows it must

76 Ibid.

77 Zhang Fang, "External Propaganda of Military Affairs in China's Military Diplomacy," *Junshi Jizhe* (*Military Correspondent*), 1 January 2012, pp. 38-40.

78 Ibid.

79 Ibid.

80 Meng Yan, "Vigorously Enhancing the Construction of the International Public Opinion Environment," *Junshi Jizhe* (*Military Correspondent*), 22 September 2011.

81 Ibid.

increase the objective understanding of the PLA by the outside world if it hopes to counter wild conjectures or rumors. It is difficult to re-obtain the initiative in public opinion once it is lost.[82]

Meng notes that media reports are the main channel through which impressions are ultimately formed; therefore, China must set agendas and carefully engineer topics of discussion in the news if it is to properly guide public opinion. Proper dissemination activities guide public thinking according to a set framework and angle, which helps to control the generation of public opinion. Meng notes this is a common convention among countries around the world.[83]

Finally, Meng states that the PLA needs to be the first to respond to incidents and provide as much information as possible if it is to gain the initiative. This is necessary, since the new media environment is characterized by limitless information capacity, fast dissemination, openness, and the interactive nature of the dissemination process. "It could be said that whoever holds the networks controls the world."[84] The PLA, in order to accomplish this mission, must strengthen its dissemination capacity if it hopes to squeeze out negative public opinion with positive information. Thus far it has constructed the MOD website (mod.gov.cn), the China Military Online (chinamil.com) website, a military affairs channel for Xinhuanet.com, and a military affairs channel for China National Radio (cnr.cn) to do so.[85]

Military Propaganda and Online Media

Hu Quanliang, the chief editor of the *Zhanyou Bao* News Agency's Internet Editing Office, wrote that the days of "I talk, you listen" are over for China with regard to the media. Now media are interactive and there is an exchange between the disseminators and the audience. Hu offered websites that differed from Meng's: China Military Forum (military.china.com), Iron Blood Forum (tiexue.net), Sina Military Forum (mil.news.sina.com.cn), and others. Such sites allow for more democracy in the media. Hu adds, however, that the military websites' propaganda content must "effectively permeate into society and cause the audience to unwittingly change its ideology and behavior, ultimately achieving a 'same frequency resonance' with the propaganda themes set up by the media."[86]

The PLA is aware that some nations are conducting public opinion warfare and psychological warfare on the Internet in order to win public opinion. Hu warns that false information can damage the PLA or cause audiences to misinterpret their actions, and adds the following:

> One small piece of news can heat up instantly through the Internet, causing individual extreme speech to proliferate into an irrational social mood or

82 Ibid.
83 Ibid.
84 Ibid.
85 Ibid.
86 Hu Quanliang, "Fighting a Good Proactive Internet Media Military Propaganda Safety Fight," *Junshi Jizhe*, 26 September 2011.

causing a local problem to expand into a universal problem, and typically these problems evolve into political problems. This requires the network sensor to pay close attention to trends in Internet expressions of opinion, and to appropriately and promptly carry out public opinion monitoring and guidance to guard against dissemination of false information on the Internet.[87]

China must work to seize the initiative in Internet military public opinion. It must establish regulatory systems that guide education, situation analysis, and integrated examination and evaluation. It must analyze network security and insure that secrets are always hidden. The dissemination of news is now an important part of real soft power. The PLA must always be on guard against the spread of false information that is disadvantageous to it. Such information can cause not only domestic but also international audiences to misjudge the PLA and its actions or intent. It is likely to harm its image as well.[88]

Military Transparency and Reporting

Pu Duanhua, a professor at the PLA's Nanjing Institute of Politics, discussed the concept of "limited opening" reporting. He defined military transparency in the following manner:

Military transparency is a process and mechanism by which a sovereign nation in a timely manner continuously opens up its military intent, capabilities, activities, and other such information in order to guard against war, control war, or protect national interests. It is essentially the same as military diplomacy and military deterrence in that they are all means of military struggle.[89]

Pu adds that any reporting that produces a negative impact on national interests, the strategic environment, the PLA's actual military strength, or other factors should have its content restricted. The content of reporting must comply with the military's objectives, it must pursue trusted sources, it must be time-sensitive, and it must abide by the military's rules of secrecy. Military reporting should implement the Party's strategic intent and oper-ational guidelines, as well as the operational command's orders and directives.[90] In short, Pu offered the following "how to" on military reporting:

The reporter must be adept at imposing measures on military incidents from the perspective of the overall situation in terms of international and domestic politics, diplomacy, and the military struggle, revealing their significant value from a political angle and relevantly and properly gathering and selecting the facts to report. The reporter must be full of fervor for praising our victory,

87 Ibid.
88 Ibid.
89 Pu Duanhua, "The Principles and Art of Military Reporting," *Junshi Jizhe*, 15 April 2011.
90 Ibid.

praising our heroes, talking about our combat accomplishments, displaying the combat style of the PLA officers and men, and molding an excellent national and military image.[91]

Military Media Confidence.

For the past two or three years, the Chinese military has acted more aggressively and confidently than at any time in the recent past. Such open confidence can be found in Chinese speeches at conferences and in open source reports prepared by various institutes. The Nanjing Institute of Politics, apparently the PLA's main theoretical center for writing on military media issues, noted that the PLA's confidence in revealing the geopolitics behind media's control of military information indicates poise. Two Chinese analysts, Ding Chunguang and Ma Gensheng, noted that "voluntarily revealing things displays a full grasp of political conditions and full confidence in national security."[92] It is indicative of the current bold PLA attitude of "looking down on all, with none daring to oppose."[93]

But the West should not be overly optimistic about the release of military information by the PLA. The same authors stated that the PLA must insist on following the principle of "letting no one know" and adding stricter controls. The rationale for this is that each geopolitical move has advantages and disadvantages. Advantages in releasing information include: advantages in producing important images, advantages in producing an important psychological effect, advantages in producing important military advantages, and advantages in producing political advantages.[94]

The Nanjing authors added another caveat to their transparency claims, which indicates the intent behind geopolitical moves. They noted that "disseminating important military information in time of peace is ultimately for the goal of influencing all relevant governments, military forces, and popular psychology to serve the needs of the nation's political benefit."[95] An ability to infiltrate during times of peace helps carry out psychological attacks and the attainment of geopolitical superiority. This means that China must possess the ability to control the way and time that "effects" appear. For example, the strategy behind the news of the first flight of the J-20 aircraft in early 2011 was crafted to announce the PLA's achievements and demonstrated military power. This caused some countries to stop considering attacks on China, in the author's opinion. Further confirmation of the "false being taken as true" can be obtained from mainstream media, where one can watch its psychological effect on the populace.[96]

In another example, to offset US exercises with China's neighbors that are (from China's point of view) war games used to intimidate and contain China, the PRC has undertaken a number of joint exercises with nations of the Shanghai Cooperation

91 Ibid.

92 Ding Chunguang and Ma Gensheng, "Effectively Controlling Lively Spokesmen—On the Control of the Dissemination of Major Military News," *Junshi Jizhe*, 15 April 2011.

93 Ibid.

94 Ibid.

95 Ibid.

96 Ibid.

Organization (SCO) and Indonesia, among others. Li Daguang, writing in Hong Kong's *Tzu Ching*, stated that exercises are a type of soft power used in a deterrent manner to influence an opponent's decisions in order to achieve one's own objectives.[97] Once public opinion is mobilized it can tilt the balance of values and postures of the international community.

Military Media's Double-Edged Sword

One challenge of the network age is that Chinese Internet users (and other users worldwide) have become the subjects of foreign military dissemination, where users act as both recipient and re-transmitter.[98] In the world of soft power, cell phones and the Internet represent a double-edged sword. Is it desirable to be transparent and act as a recipient and re-transmitter of information or is it better to adopt the policy of "letting no one know"?

Media's information technology allows trainers to expand the work accomplished in a department and also enhance the Party's influence among the troops. But media technology also allows for the spread of bad habits (gambling, hacking, etc.) among the troops and provides access points for foreign governments to penetrate PLA systems. This requires the close indoctrination of troops about both the positives and the dangers and negatives of the information age. Such training includes teaching all personnel the basics of information security and the close monitoring of their online or cell phone activities.[99]

Other analysts pointed out more limitations or disadvantages of Internet use. One article noted that PLA soldiers have been prohibited from socializing online to prevent them from divulging sensitive information to friends, especially of the international variety. The article noted that "soldiers are not allowed to use mass media for matchmaking or making friends, and are also forbidden from using the Internet outside the army without permission."[100] Soldiers also cannot watch or listen to political programs from overseas media, nor can they open their own websites or blogs or publish political information online.[101] A member of the Nanjing military community stated that "we should organize a contingent of both online commentators and influential 'individual bloggers' with personalized characteristics."[102] This contingent can "use positive information to get rid of the space for negative public opinion, apply positive viewpoints to put an end to the negative trend of public opinion, and increase the timeliness, pertinence, and effectiveness of online military related public opinion."[103]

97 Li Daguang, "China Strives to Break Out of US Containment with Overseas Military Drills," *Tzu Ching*, No. 250, 1-31 August 2011, pp. 20-21.

98 Zeng Jia, "Omnipresent External Dissemination of Military News," *Junshi Jizhe*, 15-16 March 2011, pp. 53-54.

99 Luo Xianwu, "Apply Modern Media to Carry Out Rapid and Highly Effective Political Mobilization," *Zhongguo Guofang Bao*, 18 August 2011, p. 3.

100 Fu Wen, "Soldiers Banned from Online Socializing," *Global Times* Online (in English), 1 June 2011.

101 Ibid.

102 Pu Duanhua, "Backstage Network Noise in Perspective—On Online Speculation of Military Information," *Guangming Ribao* Online, 20 May 2011.

103 Ibid.

This attitude indicates the PLA recognizes that every soldier or officer has become a netizen of China. Internet access allows all servicemen to have a place for learning, entertainment, and advice. It is a place to exchange views as well. However, *Jiefangjun Bao* has also advised that "only by taking the initiative to positively guide public opinion via the Internet can we clean the space of all noise and eliminate the influence of wrong speech."[104] The characteristics of military culture must be present to provide officers and soldiers with the correct platforms for learning and exchanging information.[105]

Military Image and the Three Warfares

Military image power is transmitted to the public through various channels of propagation that influence the public's perception and judgment of the military. Creating a good military image, from the Chinese perspective, involves obeying the CPC's commands; serving the people; ensuring the ability to fight and win; gaining the upper hand through an image of strength; and innovating an all-inclusive approach. Modern mass media, an advanced military culture, foreign military exchanges, and large-scale military activities all enable the advancement of military image, the "business card of military soft power."[106] Military image is a prerequisite for effectively wielding public opinion warfare, psychological warfare, and legal warfare as well as psychological deterrence power.[107]

The PLA's military image and control of military public opinion are manifested in the PLA's "Regulations on Political Work of the Chinese People's Liberation Army," which is a three-pronged approach. The concept consists of "three kinds of warfare": public opinion warfare, psychological warfare, and legal warfare. They represent the content of political work in the armed forces. The objective of the three-warfare approach is to win without fighting. The three-warfare approach follows a historical Chinese tactical pattern of using stratagem, diplomacy, psychological operations, and morale-related activities. In the information-age the three warfares have extended the battlefield of traditional warfare from the military front to the civilian rear and from simply soldiers to soldiers and civilians. The latter category includes hackers, according to author Xu Feng.[108]

Public opinion warfare's core objective is to "control news and public opinion" and is targeted at the local public. Legal warfare involves seizing the initiative through the attainment of justified public support, is aimed at world opinion, and provides a legal foundation for the other two warfares. Psychological warfare, in contrast to public opinion and legal warfare, is designed to lower the will of enemy forces. Some

104 Staff Commentator (unnamed), "Building New Platforms, Fostering New Skills—Fourth Commentary on Profoundly and Persistently Cultivating Core Values of Contemporary Revolutionary Servicemen," *Jiefangjun Bao* Online, 7 June 2011, p. 1.

105 Ibid.

106 Tian , Chen, and Ding.

107 Ibid.

108 Xu Feng, "Objective: Prevailing without Blood—An Analysis of the PLA's 'Public Opinion Warfare, Psychological Warfare, and Legal Warfare' Efforts," *Tzu Ching*, No. 177, 1 July 2005, pp. 86-88.

military regions have produced broadcast, pamphlet, and network-based psychological-warfare-type training. New psychological warfare units have been established and some aircraft are being remodeled as public opinion aircraft. Training personnel in public opinion warfare, combat psychology, and the law of war has begun. US activities in Kosovo, Afghanistan, and Iraq were used as examples of the three warfare techniques applied in practice.[109]

The *People's Daily* noted that public opinion warfare represents the "integrated use of newspaper, radio, television, the Internet, and other new media" in a "planned and targeted manner to achieve the goals of encouraging the combat morale of its own side," to cause the "combat will of the enemy to collapse," and to "guide international public opinion."[110] In 2004, Nanjing's Institute of Politics offered a new course on public opinion warfare, which "reflects the requirements of new military changes in the world."[111] Learning how to make contact with the news media's print and digital versions is now a required course for some cadres.

The character of future public opinion wars indicate that if high-tech devices are not absorbed and integrated into society and the military, then society can be destroyed or toppled by those who have such devices. The recent Arab-Spring events indicate that in the all-media era, public opinion can become a main battlefield for determining changes in the political situation. The PLA must learn to anticipate future developmental trends in public opinion tactics in order to successfully confront them in future scenarios.[112]

PLA analysts are studying topics such as the similarities and differences in public opinion (media) warfare and psychological warfare in order to uncover challenges to military propaganda and military soft power. Wang Lin and Wang Guibin are two such analysts. Similarities they uncovered include common strategic objectives, similar operational methods (working on people's cognitive systems), using the same mass media as their operational transport means, and using military power as a shield while relying on high-tech equipment. Differences include public opinion's non-stop efforts (during peacetime and wartime), using the war of words and a host of variables, whereas psychological operations are more focused on wartime; public opinion warfare's focus on the objects of a society and culture's structure versus psychological operations short-term focus on a soldier's will using deception and disruption; and public opinion warfare primarily using the media, whereas psychological operations use leaflets, broadcasts, and other means. The authors conclude their analysis stating that offensive operations are more effective than defensive operations in the field of information war.[113]

---

109 Ibid.

110 Wang Lin and Wang Guibin, "An Analysis of Public Opinion Warfare and Psychological Warfare," *Jiefangjun Bao* (*People's Daily*) Online, 8 June 2004. .

111 Heng Xiaochun and Zou Weirong, "New Course Added to Curriculum of the PLA's Nanjing Institute of Politics,"*Jiefangjun Bao* Online (www-Text), 22 March 2004.

112 Song Mingliang, "Research on Building Up Technology and Equipment for Public Opinion Warfare in the All-Media Era," *Junshi Jizhe*, 15 May 2011.

113 Wang Lin and Wang Guibin, "An Analysis of Public Opinion Warfare and Psychological

As a result of such findings, public opinion warfare has also been integrated into other departments usually associated with a specific issue. These departments include the Research Institute of Psychological Warfare, the Research Institute of Military Intelligence, the Research Institute of Ideology and Culture, and the Research Institute of Political and Ideological Work of the Army. The simulation of actual combat is included in one department as a teaching method.[114] Another source stated that "Appropriate cultural battle simulations must be developed to accumulate the necessary information and experience to improve one's own defensive abilities in media warfare."[115]

Conclusion

Information technology advances have forced Chinese experts to focus more intently on the advantages and disadvantages of high-tech media devices. The results of external Arab-Spring-type events and internal Jasmine Revolution efforts within China have accelerated the pace of the government's involvement and concern. This is not to suggest, however, that the concept is new to the Chinese. They have been theorizing about the use of high-tech media for the past several years. They believe that in peacetime and wartime, media conflict or public opinion warfare is being conducted by nations around the globe and that China must be on guard to defend itself against them.

One analyst stated that "information technologies have equipped the side with information advantages with the capability to promptly, accurately, and sufficiently deliver public opinion warfare information to targeted areas and people at a desired time and place."[116] Not only is the government involved in such activities, the analyst adds, but so is the civilian population. They conduct "thumb public opinion warfare" since they can manipulate their video, conversation, text, web surfing, and picture-taking cell phones just by moving their thumbs.[117] Some Chinese experts now consider supremacy in information control to be the core aspect of public opinion warfare under informatized conditions. Public opinion warfare, they note, has economic, political, and cultural aspects that can act as deterrents to aggression.

The reason that activities such as deterrence and deception are more successful than in the past is due to the properties of the Internet and the digital age. Issues are spread faster and farther and reach a much wider audience than in the past. Wartime targeting is enhanced by sampling a population's feelings and rationale via the net in peacetime. Several Chinese media experts even believe that at a strategic level there is no difference between peacetime and wartime media. In both cases there are attempts to affect the subjective judgment of members of a society. The use of multiple sources

Warfare," *Jiefangjin Bao* Online, 8 June 2004.

114 Song.

115 Wang Lin, Wang Yitao, and Wang Guibin, "A Study on the Strategy of Cultural Effects in Media Warfare," *China Military Science*, No. 6 2005, pp. 120-128.

116 Zhang Changjun, "Study on Command Confrontation in Propaganda Warfare under Informatized Conditions," *Junshi Jizhe*, June 2007.

117 Ibid.

can add weight to the process of convincing individuals or groups of a concept.

The book *Information Security: Threats and Strategy*, edited by Zhang Xinhua, contains a call for new strategic thinking. It states that "the concept of information strategy and the ideas, values, norms, and ethics expressed through various media strengthen and unleash the effects of soft power."[118] Further, "the key to success may be in proficiently practicing strategic management of information capabilities. Thus what lies at the heart of grand strategy is paying attention to information security and building and applying information strategy."[119]

Zhang thus recommends that China prepare a new grand strategy, with information at the center of attention. Two areas of this strategy are the science and technology area (security and safety of digital space, and perhaps the autonomous infiltration into foreign systems); and the political area, where soft power rules. In Zhang's opinion, opportunities abound to improve or exploit information sovereignty, information hegemony, information permeation, information domination, and information contamination, among other issues.[120] A new test of strength will be a country's ability to destroy or manipulate information flows, since nations now rely so heavily on such flows. Strategic goals "can be achieved by destroying or manipulating the flow of information on computer networks to destroy an enemy's telephone networks, oil pipelines, power grids, traffic management systems, systems for transferring state funds, systems for transferring accounts, and healthcare systems."[121]

China, like Russia, is attempting to deter the US through international efforts focused on alliances that put roadblocks in the path of further cyber developments. These efforts are also gaining momentum. In the past two years, the Chinese and Russians have begun cooperating on cyber issues through the Russian initiated forum in Garmisch, Germany. In 2011 the Chinese hosted the forum for the first time on their soil. This effort expands on those the Chinese have participated in at the United Nations and through the Shanghai Cooperation Organization. The *Internet White Paper* discussed the spread of the Internet and mobile phones in China.

Of course there are many problems associated with using high-tech media in such a manner. First, it is very difficult to establish tight control over an influence campaign, since there are so many wild cards in play. Individuals or groups who may have nothing to do with the campaign's target or eventual goal can play. Second, the use of a concept such as using what is false instead of what is true could backfire on the campaign's creator if the wrong intention is taken by one's domestic audience. A good example of wild cards influencing public opinion is the train crash near Wenzhou, China, in July 2011. The Central Propaganda Department issued instructions regarding what journalists could and could not report. Unfortunately for the CPC, the unofficial reporting and photos of bloggers at the scene (there were people on hand with mobile devices, etc.) produced an entirely different story than newspapers were reporting. Bloggers poured criticism

118 Zhang Xinhua, editor, *Information Security: Threats and Strategy*, 2003, p. 52.
119 Ibid., p. 53.
120 Ibid., p. 54.
121 Ibid., p. 48.

on the authorities and eventually caused the Central Committee of the Communist Party to issue a circular calling for more transparency about accidents.[122]

However, in the end, China's recognition of the importance of information flows as being at the heart of grand strategy indicates that public opinion, both internal and external, will remain a focal point into the foreseeable future. The CPC appears destined to try to erect sturdy structures and firewalls around the minds of its citizens while trying to penetrate the firewalls and minds of people abroad.

122 L. Gordon Crovitz, "Beijing's Crash Course in News Censorship," *Wall Street Journal* Online, 8 August 2011, at http://online.wsj.com.

CHAPTER TWO
CHINA AND INFORMATION DETERRENCE

Introduction

Ever since the 1990s, the topic of information deterrence has occasionally been included in conferences designed to discuss information warfare (IW) topics. American, Russian, and Chinese authors all wrote on the concept and not always in theoretical agreement. Inevitably, comparisons were made to the theory of nuclear deterrence, which has dominated strategic thought for the past fifty years.

At times the discussion took strange twists and turns. For example, in 1995 a Russian theorist offered an unusual scenario with an unexpected outcome. This theorist stated that if the US, with its information dominance, initiated an information attack against Russia's weak information infrastructure, then Russia would respond not with an information attack but with a nuclear weapon.[123] That is, the threat of a nuclear holocaust would be used as an "information attack deterrent" in place of Russia's lack of an information attack capability.

Today, some fifteen years later, many nations across the globe are more assured about the strength of their information infrastructure. As a result, the issue of information deterrence is undergoing a reexamination worldwide. The discussion has broken into several parts in some forums, such as the legal, media, and cyber aspects of information deterrence. The disparity in digital capabilities among countries has not disappeared completely, however. Clearly one size does not fit all in the evolving age of digitalization and miniaturization.

This chapter will discuss how China and the US have reconsidered the use of the information deterrence concept. It is divided into two parts. First, it will discuss the emerging concept of information deterrence in China more closely. For China the concept is an extension of its peace activist agenda. Second, it will briefly look at the short history of information deterrence from the vantage point of American authors. The conclusions will examine what changes these emerging issues reveal for the concept of deterrence in general. Will it result in a new definition, in the institution of defined caveats (such as the extended and limited deterrence concepts that evolved in the nuclear age), or in the elimination of the concept of information deterrence in general as some think it should?

Chinese Views on Information/Cyber Deterrence

The Chinese have written on several issues related to the concept of information deterrence. This section will first examine Chinese definitions of deterrence, strategic

123 V. I. Tsymbal, "Kontseptsiya 'Informatsionnoy voyny'" (Concept of Information Warfare), speech given at the Russian-US conference on "Evolving Post-Cold War National Security Issues," Moscow 12-14 September 1995, p. 7.

deterrence, and information deterrence. It will then look at the development of the information deterrence concept in China's military.

Definitions

A check of the 1997 *Chinese Military Encyclopedia* revealed no entry for the term "deterrence." An entry for the term "information warfare" in the same encyclopedia noted that "Psychological operations influence the enemy's understanding and decision-making systems by information propaganda, information deception, and information deterrence, thereby in essence breaking down one kind of the enemy's information operations."[124] Thus the term is used in other definitions (even jointly with the word "information") but not defined separately.

Editors Peng Guangqian and Yao Youzhi defined deterrence in their excellent work *The Science of Military Strategy* as "military conduct of a state or a political group in displaying force or showing the determination to use force to compel the enemy to submit to one's volition and to refrain from taking hostile actions or escalating the hostility."[125] Deterrence requires a deterrent force able to impact the overall strategic situation; the determination and volition to use the force; and the ability to make an opposing force perceive and believe these prior two points.[126]

The military action of strategic deterrence is defined as "the strategic move taken by a state or a political group for the purpose of forcing the opponent to submit to one's volition in the overall war situation through showing force or the determination of preparing to use force."[127] What strategic deterrence values most is momentum from military preparation, from showing a disposition of strength to an enemy, and from military strikes.[128] Thus, the creation of momentum, or *shi*, is a valued commodity of a deterrence concept or means of deterrence. *Shi* can also be interpreted as energy or strategic advantage. It is the latter concept that deterrence strives to attain whether through physical (force development and deployment) or mental (development of fear of retribution in an opponent).

Information deterrence is defined in *The Science of Military Strategy* as "the deterrence that depends on the powerful performance of information science and information technology, and it is put into effect by the momentum and power of information warfare."[129] In the world of information, the creation of deterrence from

124 *Chinese Military Encyclopedia*, Supplemental Volume, 1997, p. 527.

125 Peng Guangqian and Yao Youzhi, editors, *The Science of Military Strategy*, English Edition, The Military Science Publishing House, 2001, p. 213.

126 Ibid., pp. 213-214.

127 Ibid., p. 222.

128 Ibid.

129 Ibid., p. 220. In a glossary at the back of the English language translation of *The Science of Military Strategy*, a translation the Chinese themselves provided, the term cyber is equated to the term informationization. That is, the same Chinese symbol was translated as "cyber, informationization." For that reason, this author sees little difference in cyber deterrence and information deterrence. The terms are used interchangeably hereafter.

momentum is accomplished via the preparation of cyber power, showing an enemy force a disposition or capability of cyber strength, and from actual cyber strikes (perhaps the numerous computer reconnaissance activities of the Chinese).

Information deterrence, according to Peng and Yao, has the following features: first, permeability or the ability to permeate not only the military but also politics, the economy, culture, and science and technology; second, ambiguity, where the difference between information deterrence and information offense is hard to distinguish; third, diversity, such as unauthorized visits, malicious software, database disruption, etc.; fourth, two-way containment, where victims of an information attack may not be just the enemy but also others, to include oneself, due to the interconnectedness of networks and the global grid; and finally, the use of People's War as a capability, that is, the potential of people joining in to combat an enemy on the net.[130]

The Science of Military Strategy also notes the following points which apply more to the transmission of information ("information transmission is the necessary condition for creating the deterrent impact of strength and determination"[131]) in order to impact the cognition of an opponent:

> Deterrence requires turning the strength and the determination of using strength into information transmitted to an opponent, and to impact directly on his mentality in creating a psychological pressure to shock and awe the opponent…for this reason, effective strategic deterrence depends not only on strength and determination, but also on the above-mentioned information acquired by the deterred side. If the opponent has not acquired the above information or the information acquired is not accurate, or the deterred side believes that the acquired information is only bluffing and intimidation, then it cannot create creditable and effective strategic deterrence…only when the opponent on receiving deterrence information perceives and believes that if he acts rashly, he may suffer a more severe punishment, can the deterrence obtain the expected impact.[132]

Finally, Peng and Yao write that deterrence seeks momentum in several postures: creating momentum through military preparation, demonstrating momentum by showing one's disposition of strength, and augmenting momentum with military strikes.[133]

Zhao Xijun, writing in *China Military Science* in 2001, defined deterrence as "military actions in the form of a show of force between countries or political groups, or an indication of their resolve and readiness to use force, intended to make an opponent not dare to take hostile action or to escalate his actions."[134]

130 Ibid., pp. 220-221.

131 Ibid., p. 215.

132 Ibid., pp. 214-215.

133 Ibid., p. 222.

134 Zhao Xijun, "Victory without War and Modern Deterrence Strategy," *China Military Science*, issue number is unknown, 2001, pp. 55-60.

The 2004 Chinese book *New Concepts during Military Transformation*: *Interpreting 200 New Military Terms* defined several deterrence-related terms, to include the strategy of deterrence, strategic deterrence, nuclear deterrence, space deterrence, forward deterrence, full spectrum deterrence, and, most importantly, information deterrence. The latter term was defined in the following way:

> With the backing of information weapons, intimidating and containing an adversary by threatening to use information weapons or when necessary carrying out an information attack. Information deterrence is essentially warning an adversary in advance about the possibility that information weapons will be used or information attacks will be carried out, as well as the serious consequences these actions may give rise to, causing the adversary to weigh the pros and cons and thereby producing psychological fear, forcing him to submit to the will of the side carrying out deterrence or abandon his original plans and thus allowing the side carrying out deterrence to achieve certain political objectives.[135]

In 2009, Central Military Commission member General Jing Zhiyuan stated that in the 21st century, strategic deterrence must be built up with the construction of "information-technology-dependent strategic missile forces."[136] In this case the amount of information technology built into modern systems indicates the deterrent capability of China's strategic force.

In 2010, Senior Colonel Yao Yunzhu, writing in the US journal *Air & Space Power*, stated that China will continue to apply deterrence at the grand strategic level while depending more on "uncertainty" for a better deterrence effect.[137] Even though her comments were with regard to nuclear deterrence, they could also fit an information deterrence scenario. In the age of computer hacking, "uncertainty" as to a hacker's actual identity or government connection is a huge problem.

Other terms that may develop in Chinese thought would be political, economic, or even cultural information deterrence. The latter term could be interpreted as the cultural or soft power offensive described in Chapter One. Economic information deterrence would be a concept to fear based on the amount of US debt that China currently owns. If a nation controls or manipulates economic information to a significant degree then it may be capable of implementing a type of economic information deterrence. This means a nation could deter another nation simply based on the former's control over the latter's economic assets.

Deterrence in Chinese Thought

If one were to attempt to extrapolate what China's cyber deterrence theory might

---

135 National Defense University's Scientific Research Department, *New Concepts during Military Transformation: Interpreting 200 New Military Terms,* PLA Publishing House, 2004, p. 108.

136 "'Strategic Deterrence' Enhanced in the Information Age, Top Nuke Generals," *Xinhua*, 2 February 2009.

137 Yao Yunzhu, "China's Perspective on Nuclear Deterrence," *Air & Space Power Journal*, Spring 2011, p. 30.

look like from its strategic deterrence theory, Lieutenant General Zhao Xijun's 2001 article on the topic of deterrence in *China Military Science* is an interesting contemporary start point. Zhao, a deputy commander of Second Artillery (responsible for nuclear weapons), implies that deterrence theory is based on a combination of stratagems. These stratagems are using soft power and reconnaissance to win victory without war; and winning victory before the first battle. To Zhao, these specific formulations of the concept of deterrence theory in military thought come from the early works of Sun Tzu.[138]

Zhao notes that key factors in Sun Tzu's writings that influence contemporary deterrence theory include having superior military power, being fully prepared for war, having severe measures of punishment at one's disposal, having superb skill at "attacking strategy" and "attacking diplomacy," and making one's ideology of deterrence be a lynchpin in a more complete system. The essence of deterrence is to resolve war with non-war measures. Western warfare is, in Zhao's opinion, very different conceptually than Chinese warfare. He feels Western theory is based on using war to achieve political objectives.[139]

A Chinese deterrence warfare strategy protects national interests, ensures that a nation's economy, science, and technology develop quickly, and offers the nation an invincible position in complex environmental and international disputes. Zhao adds that a counter-deterrent capability is the most effective method to stop the aggressive attempts of powerful nations from harming China's national interests. Flexibility and effectiveness are other important principles for the use of deterrence, which reflects the strategists' resolve, the manifestation of military strategy, and the embodiment of power. The key factors of deterrence must be cleverly assembled, flexibly mobilized, and securely developed to enable the ideal strategic outcome.[140]

First, a proper deterrence strategy includes the ability to judge the hour and to size up the situation while cautiously making decisions. Do what suits the time and place and coordinate actions. A nation must have a good grasp of the target and the objective of its deterrent posture. Here the US must wonder if all of the hacker attacks attributed to China are nothing more than an attempt to size up the target, to map the US infrastructure in order to spot vulnerabilities. The correct time and judgment must also be used when attacking an alliance. Initially it is necessary to attack those countries with weak social and political foundations. These actions warn others and create a chain reaction of fear in the alliance.[141]

Second, Zhao notes that China should use an integrated deterrence approach. A single deterrent force is not sufficient to constitute effective deterrence. Comprehensive power must be employed to retain the strategic initiative. Third, it is necessary to combine truth with falsehood, a direct application of stratagems. This combination can work to awe an enemy force into submission. Friendly forces must look for

138 Zhao Xijun.
139 Ibid.
140 Ibid.
141 Ibid.

opportunities to attack an enemy forces power and resolve. It must create a posture of deterrence through a policy of truth and falsehood to deprive an enemy of will power. When striking, it must do so resolutely, threatening targets with the greatest strategic value first, those the enemy does not want to see hit. Finally, psychological offense and strategy are the best tactics to gain victory. Deterrence is a test of power and resolve and a test of strategy and wisdom. When there is no smoke or gunpowder, strategy acts as a multiplier of power and resolve in deterrence. Strategic thought evolves and develops continuously along with societal developments, especially as changes occur in the military sphere.[142]

> No matter what type of deterrence is used
>
> Its ultimate outcome is never merely the result of a comparison of the relative power of the two opponents. More important is the result of an analysis of the benefits which the deterring side and the deterred side might secure, of the price they each might have to pay. Implementing deterrence requires stepped up research of the threat the country faces. It requires scientific analysis and judgments.[143]

An equally interesting article on strategic deterrence was published in 2004 in the same journal. Zhou Peng and Wen Enbin, from the Academy of Military Science, wrote that strategic deterrence refers to a "country or political block's military actions to compel an adversary to not dare take hostile action or escalate actions through a show of force or indicating the resolve of being prepared to use force, thereby achieving specific strategic goals."[144] The possession of military strength is a prerequisite along with the resolve to use force and the ability to make the one being deterred aware of your capabilities. Now, informatized warfare under conditions of nuclear deterrence can have tremendous deterrent power capable of achieving strategic objectives. Targeted deterrence can be achieved due to the controllability and flexibility of informatized measures. For example, in the Iraq War, the US targeted the Iraqi military with soft components. The US military achieved psychological deterrence as it showed off new weapon capabilities; intentionally "leaked" strategies and tactics; conducted strategic and tactical deception; permitted selected media to be involved in the war process; and maximized the threat effect.[145]

Former Chinese President Jiang Zemin recommended elevating deterrence to the level of strategy, according to Zhou and Wen. It should be used to contain war, delay its outbreak, or prevent its escalation. The core of new deterrence capabilities should be "assassin's mace" type technologies. Jiang emphasized mobilization measures as a

142 Ibid.

143 Ibid.

144 Zhou Peng and Wen Enbin, "Developing a Strategic Deterrence Theory with Chinese Characteristics," *China Military Science*, No. 4 2004, pp. 19-26.

145 Ibid., pp. 20-21.

priority development. Due to the fast nature of high-tech wars, a war's start can have decisive significance. For that reason China "must establish an emergency mobilization combat force" as well as a strong traditional force capable of imposing deterrence in the strongest manner. In this way China can confidently unleash the deterrent effect of People's War under high-tech conditions.[146]

It is only through comprehensive national strength, in Zhou and Wen's opinion, that a reliable deterrent effect can be generated. This image of strength is particularly important to construct during the so-called 20 year window of strategic opportunity that China envisions before it. Strength should be built around nuclear forces; the close integration of information resources, space resources, and conventional forces; and the People's War concept under high-tech conditions. A good deterrent force involves the use of nuclear deterrence, conventional deterrence, space deterrence, and information deterrence.[147] It also requires effective reserve forces and adaptable strategic industries.[148] The authors add that

> There are no fixed models for strategic deterrence…different deterrence forms must be imposed based on the different properties of the deterrence objects and deterrence objectives by putting forth effort to look for weaknesses and 'points of penetration.' The acme of the art of strategic guidance is fully reflected in the proper selection and constant innovation of deterrence forms; it is the most real, most dynamic part of wielding strategic deterrence.[149]

Information deterrence

There have been a series of articles and interpretations of information deterrence over the past decade. This section highlights some of those interpretations. In 1999, Chinese author Shen Weiguang, the father of IW in China, wrote that the main IW battlefield will be intangible, information space, and this will cause a change in the state of war. The effect of this change will include the softening of strategic objectives, the development of information deterrence as a new means of deterrence, the determination of military actions by the possession of information, the rising status of Special Forces, and the use of civilians on the battlefield.[150]

Authors Lu Xiuru and Yu Zhengxue, also writing in 1999, noted that intellectual information deterrence would be part of the intellectual-economic era that had descended on the world. This era will change the form of war and no longer make violence necessary.[151] A 2000 article by the noted Chinese stratagem specialist Li Bingyan stated that "future war will be a high-technology war within the framework of

146 Ibid., pp. 22-23.

147 Ibid., p. 24-25.

148 Ibid., p. 26.

149 Ibid., p. 25.

150 "Chapter Two: The Third World War—Total Information War. The Views of Chinese IW Specialist Shen Weiguang," in *Dragon Bytes*, 2004, p. 35.

151 Lu Xiuru and Yu Zhengxue, "Forecasting the Trend of War in the Era of an Intellectual Economy," Beijing *Jiefangjun Bao*, 6 April 1999, p. 6.

nuclear deterrence and information deterrence."[152]

Zhao Xijun, in his 2001 article mentioned earlier, adds that the deterrent roll of advanced weaponry is increasing, a direct link to the use of digital weaponry. Further, if China is able to capture the strategic information resources of a country, then it can "win victory before the first battle." It can check an opponent's behavior using non-war methods. In the past, China has referred to the US as a cyber hegemonic power. To attack this process, China should engage in active and effective deterrence. Power is the key factor in deterrence strategy. Enemies must be made to feel that their actions will lead to consequences where the losses outweigh gains.[153] Thus, extrapolating, China must develop into a cyber power if it is to develop the proper counter-deterrence ideology required to put up a unified fight. If military power is the main deterrent component of comprehensive power, then cyber power cannot follow too far behind. Cyber power is most likely now considered as a main ingredient of comprehensive power computations that the Chinese update regularly. China cannot utilize information deterrence if it is not a cyber power. As a cyber power, China can attempt to exploit foreign information resources, as it is apparently trying to do, as it procures terabytes of information from foreign nations' information systems.

China has continued to conduct reconnaissance activities against the US and many other nations, ignoring repeated calls to cease such actions. Interestingly, Zhao offers a piece of advice in his article that could be used by US policy makers to counter these reconnaissance activities. Zhao writes

> If the opponent persists in having his own way and refuses to stop his hostile actions, then the other side must select the right time and an appropriate objective and execute high-intensity deterrent actions against the enemy, to include a warning strike. This is to demonstrate full and resolute determination to fight the enemy to the end, and force the enemy to abandon his high-handed scheme.[154]

Of course, a "warning strike" would likely be in the form of a cyber attack against a key utility or bank or military communication network and would hopefully not include missile strikes leading to further escalation scenarios.

A 2002 article in *Jiefangjun Bao* stated that information deterrence will make warfare more transparent.[155] So far, however, cyber activities have been most often characterized as anonymous. The difficulties associated with uncovering identities are actually roadblocks to transparency.

In 2003 editor Cai Cuihong's book *Information Networks and International Politics*

152 Li Bingyan, "Recognizing One's Own Historical Place in the Flood Tide of Reform: Written on the Conclusion of Discussion of the Topic, 'Is Warfare Gradually Softening?'" *Jiefangjun Bao*, 26 December 2000, p. 6.

153 Zhao.

154 Ibid.

155 Xu Guanhua, "S&T Development Impacts All Aspects of National Security," *Jiefangjun Bao*, 22 May 2002, p. 9.

proposed an information deterrence theory. The theory postulated that soft power's use in complex events is just like using the threat of weapons and has become a core source of state power. Whoever has the ability to open its information umbrella will become the strongest power in the system. If one can control information supremacy then information deterrence can be used to make an adversary lay down his weapons. If soft power does not work, then its use in conjunction with precision-guided weapons can help achieve the goals of deterrence.[156] This argument implies that soft power is the preferred method of winning an information deterrence engagement.

The information umbrella is viewed in Cai's work as more utilitarian than the nuclear umbrella. The umbrella must be able to control information dominance and enable one side to see the adversary, while not allowing the adversary to see friendly activities. Control over information has become a new deterrent force as a result. Cai's work notes that "the side that controls information can manipulate the start and conclusion of wars, can use informatized weapons to paralyze enemy weapons and command systems, and can destroy the enemy's precision guided weapons."[157] Information control appears to be a key aspect of a deterrent force according to this explanation.

If one side possesses the capability to destroy or weaken an adversary's information resources then the other side dare not act hastily. Herein lies one of the strongest arguments in support of information deterrence in Cai's opinion.[158] However, a few pages later it is stated that "information network warfare under conditions of nuclear deterrence will be the new form of future international conflict."[159] This argument causes one to reminisce about Russian V. I. Tsymbal's 1995 statement mentioned in the introduction to this chapter. Not much has changed over the years if this proves to be the case.

Network warfare includes network spy warfare and network attack and defense warfare. It is a form of fighting similar to IW in the opinion of the work's authors.[160] Network warfare is low cost, full of surprises and anonymity, involves low personnel casualty costs, and is asymmetrical The latter concept indicates that warfare could be conducted between countries, between countries and organizations, between countries and individuals, between organizations, between organizations and individuals, and even between individuals.[161]

Cai notes that computer network warfare's basic characteristics are that "computer network space is the battlefield, computers are the primary weapons, smart programming codes are the ammunition, and personnel with computer attack and defense skills make up the operational units and detachments."[162] Capturing and maintaining network information dominance in the economic, military, and diplomatic fields are important

156 Cai Cuihong, *Information Networks and International Politics*, 2003, p. 163-164.
157 Ibid., p. 165.
158 Ibid.
159 Ibid., p. 172.
160 Ibid., p. 173.
161 Ibid., p. 176-177.
162 Ibid., p. 174.

strategic, campaign, and tactical operational goals for attack and defense scenarios.[163] Further, the mission has changed:

> The goal of computer network warfare is no longer annihilating the enemy and preserving oneself; rather, it is controlling the enemy and preserving oneself. What we call control is mainly influencing the thinking and will of the war decision-makers, putting the adversary into a darkroom, depriving him of the means for 'knowing himself and knowing the enemy,' and making it impossible to turn war potential into actual capabilities for engaging in war.[164]

The combat strength of China's armed forces will be balanced on the basis of its computing power, communications capacity and reliability, real-time reconnaissance capabilities, computer simulation capabilities, and other information elements. These elements can deter through misconceptions and psychological pressure. Without a distinction between front and rear, wars will truly become "People's Wars" and their shape could be strongly influenced by invisible information space.[165]

In 2007 Major General Li Deyi stated that information deterrence will rise to a strategic level close behind nuclear deterrence. New and important modes of deterrence will include information-technology deterrence, information-weaponry deterrence, and information-resource deterrence. Further, information deterrence and counter-information deterrence will be part of China's new mode of thinking.[166] Also in 2007 Senior Colonel Deng Yifei wrote that information deterrence would be a means, behind nuclear deterrence, to achieve national strategic goals and military strategic goals. Deng added that information has become the core concept in military thinking. Vying for information supremacy and forming information deterrence capabilities are key areas of current military thought.[167]

In 2009 a few top nuclear generals in China wrote on information resources and the information components of weaponry as they apply to information deterrence. The generals noted that information technology-dependent strategic missile forces are ways to enhance strategic deterrence,[168] a thought very similar to that of some Russian analysts. Other authors note that Sun Tzu's ideas of winning without fighting and eliminating opposing armies are nothing more than a combination of deterrence and combat theories as a new operational context that utilizes informatized (high-tech) conditions. For example, author Zhou Fangyin noted that the concept of information deterrence is defined by forcing an adversary to lay down his weapons by demonstrating

163 Ibid.

164 Ibid., pp. 177-178.

165 Ibid., p. 178.

166 Li Deyi, "A Study of the Basic Characteristics of the Modes of Thinking in Informatized Warfare," *China Military Science*, No. 4 2007, pp. 101-105.

167 Deng Yifei, "A Revolution in Military Thinking in the Information Age," *China Military Science*, No. 6 2007, pp. 71-78.

168 "Top Nuclear Generals: 'Strategic Deterrence' Enhanced in the Information Age," 2 February 2009, as downloaded from http://english.peopledaily.com.cn on 4 September 2009.

or highlighting friendly force weaponry's advanced precision under informatized conditions.[169] In turn, the demonstration provides a deterrent effect on the activities of potential adversaries.

Further, some Chinese see a close link between information deterrence in both the technological and psychological arenas. Information deterrence works best, these authors write, if the two are integrated, that is, if an effective media campaign supports the potential elimination of important strategic targets. Other Chinese writers tend to emphasize that cyber deterrence includes both the concept of winning without fighting via legal and media (persuasive) means and the concept of using actual force, which is winning under informatized conditions through the use of cyber-based precision-guided weaponry, satellite communications, and so forth. While the former attacks cognition and political will the latter attacks military means. Both can attack decision-makers. A combination of cognitive deterrence and combat deterrence appears to be the desired focus of China's cyber deterrence concept, with the desired blend or balance up to strategists. It is thought that this focus on the use of deterrence includes both civilian and military cognitive and physical targets.

Jiang Yong, in a 2010 article in *Quishi* (a semiofficial journal of the Communist Party of China's Central Committee), discussed the issues of cyberspace and cyber deterrence. Cyberspace was defined as

> A network consisting of the interconnected computers, satellites, cables, and various types of information terminals. It connects political, military, business and trading, financial, and transportation entities in all trades and industries, including governmental and non-governmental organizations, enterprises and individuals, and thus shapes the 'nerve system' on which the contemporary world and all sovereign states rely for normal operation.[170]

Cyberspace contains a massive volume of information that is used to spread a user's influence, which can be either benevolent or extremist or a combination of both. Information flows have become a strategic resource in China's opinion. China worries about US hegemony in cyberspace since the latter controls ten of the worlds thirteen root servers and thus information flows. If alterations are made to information in the servers or deception is used here, it can provide the US with the power to control the information resources of another nation. China believes the US also controls the Internet through the Internet Corporation for Assigned Names and Numbers (ICANN), which assigns domain names and digital addresses.[171]

Cyber deterrence was not defined in the article. However, as with concerns over cyberspace, Jiang highlighted US developments. He stated that US policy makers exaggerated the cyber threats emanating from China and Russia in order to increase

169 Zhou Fangyin, "The Effect of the Information Revolution on Military Affairs and Security," Beijing *Xiandai Guoji Guanxi*, 1 August 2001, pp. 28-32.

170 Jiang Yong, "Cyberspace: an Invisible New Battle Domain," *Qiushi*, No. 13, 1 July 2010.

171 Ibid.

its cyber security investment, upgrade its technologies, raise cyber war readiness, and gather momentum for cyber deterrence. Interestingly, changes in the PLA's cyber infrastructure and plans accomplished the same goals. These included setting up a cyber center (renaming the communications department of the General Staff as the informationization department), setting up a cyber security office for the National People's Congress, recruiting computer experts (People's Liberation Army-sponsored hacker competitions, etc.), carrying out cyber exercises (cyber Blue Force), developing foreign propaganda (Confucius Institutes, etc.), and including information technology corporations (Huawei, etc.) in government activities. Information superiority, Jiang concludes, is becoming the key factor in determining future calculations of comprehensive national power.[172]

There was a dissenting Chinese opinion on the topic of information deterrence. Tang Lan and Zhang Xin, speaking at a US conference in 2010, stated that the anonymity, global reach, scattered nature, and interconnectedness of information networks reduce the efficacy of cyber deterrence and render it useless. Further, the authors feel that the "potential for indirect damage is the primary problem with cyber deterrence."[173] The greatest obstacle to cooperation is "the reluctance of states to budge on their perceived cyberspace interests or differences they have in terms of laws and politics."[174] Tang and Zhang believe China has tried to improve conditions for cooperation. The country has built cyber security mechanisms with several alliances and individual countries, such as the Shanghai Cooperation Organization, the United Kingdom, the China-US Internet Forum, the China-Japan-Korea Information and Communications Ministerial, and others.[175] It is not clear why this opinion differed so drastically from the other opinions surveyed for this concept. One key factor could be that this was a presentation for a foreign audience while the other opinions were for domestic Chinese consumption.

US Views on Information Deterrence

Several Americans have worked on the topic of information deterrence. Three American works shaped the early discussion. They were produced by Richard Harknett, the duo of Richard Hayes and Gary Wheatley, and Roger Barnett between 1996-1998. Later, between 2008 and the present time, Stephen Korns, Charles Williamson, Marc Grossman, Harry Raduege, John Arquilla, and Martin Libicki were just a few of the individuals who thoughtfully brought more creativity and insights to the concept.

Richard Harknett wrote one of the very best articles on the topic of information deterrence. Harknett's background as a professor of international relations included writing chapters for books on conventional deterrence theory and nuclear proliferation. Thus, he was well versed in the general concept of deterrence from his previous work.

172 Ibid.

173 Tang Lan and Zhang Xin, "The View from China: Can Cyber Deterrence Work?" from *Global Cyber Deterrence: Views from China, the US, Russia, India, and Norway*, East-West Institute, April 2010.

174 Ibid.

175 Ibid.

Harknett defined cyber war as the preparation and conduct of military operations against military connectivity, the latter being the most important element, in his estimate, of cyber conflict.[176] A nation's connectivity must be substantial and impervious to disruption if it is to be respected and feared by an opponent. If connectivity is buttressed through redundancy, and the opposing side has similar information systems, then cyber deterrence may work. The problem, however, is how does one ascertain if this is so? With nuclear weapons, explosive force and test launches can be measured by an opposing side and a deterrent effect realized. This is not currently the case with information deterrence concepts. How does one put on a "demonstration" of a network's reliability? Does one nation "steal" something from another nation and then "show" what it took to demonstrate capability?

Harknett described several of the underlying precepts of deterrence and provided the reader with food for thought regarding how those precepts are affected by information-age developments. He noted that deterrence requires the following:

- The capability to inflict retaliatory cyber costs must be perceived as reliable.
- Deterrence requires that each side know the other's national objectives and commitment to the issue in dispute. The economic, political, and military resources available to support such commitments and objectives must be shared with one another. In the information age, this requires sharing information about networks and cyber attack options.
- Deterrence can fail due to rationality if costs of a military action do not exceed benefits and if a challenger miscalculates about threatened costs. In a virtual world such as the current cyber environment, is rational decision-making possible? Hardened concrete silos with missiles, whose intent is clear, are not the issue but rather measuring the "intent" of electrons passing through circuits. Time is not measured in terms of launch warnings and missile distance/interceptability but in terms of milliseconds, prompting instantaneous responses with little time for shared information or rationality if/when under attack.
- Deterring war through the use of conventional weapons armed with information technology can lend moral support to nuclear non-proliferation policies by reducing reliance on nuclear weapons and arguing for others to do the same.
- Deterrence models are less useable in the information age than are models of offensive and defensive cyber warfare capabilities. Harknett points this out for two reasons: first, he wonders whether a cyber attack that kills no one and reduces no buildings to rubble can be considered as a credible risk that would dissuade a state from "contemplating such an attack." Second, he notes that, at this point in time (1996, when the article

176 Richard Harknett, "Information Warfare and Deterrence," 1996, downloaded from Phil Taylor's Web Site at http://ics.leeds.ac.uk on 4 September 2009.

> was written), the question of who initiated a cyber attack still cannot be ascertained with any certainty. Deterrence rests on the assumption that an adversary be identifiable, which may not always be possible with a cyber attack. The issue of "contestability" over who initiated an attack may not be enough to prevent an attack, thereby ruining the deterrence application to cyber attacks.[177]

In his conclusion, Harknett stresses that "the nature of net war and cyber war lend themselves to analytical frameworks and a strategic calculus dominated by offense-defense models rather than by deterrence…Attempts to simply roll information warfare into strategic approaches in which deterrence is the primary concern miss what is distinctive about this new form of conflict—the contestability of connectivity."[178] Connectivity has been overcome by secret access. How to keep viruses out while connected is a new challenge.

Authors Richard Hayes and Gary Wheatley wrote an article that was based on a workshop that included IW deterrence issues. Their article stated that deterrence is "part of IW only when the attacker is known (or can be discovered), the defender has a credible capability to threaten important interests of the attacker, and the attacker cannot defend those interests. Participants argue that a visible set of defenses is the beginning point for deterring attacks on important computer systems."[179]

The authors divided IW deterrence into two parts, cyber-war attacks and media warfare attacks. Their division is much like the Russian understanding of IW, whose two aspects are information-technical and information-psychological. Cyber intrusions occur every day against US targets. Some are more heinous than others due either to their sophistication or to their backing by a nation-state. Cyber penetrations can take two forms: intrusions of computer systems by other computers or intrusions of computer system elements as part of a physical destruction plan. Media warfare can involve sophisticated media campaigns or the communication of inaccurate images to selected publics. The goal of media-warfare attacks is to lower the morale of both an adversary's military and civilian population and to throw doubt into the minds of the constituency.[180]

In this sense, deterrence will be limited to "rendering an adversary ignorant, poor, uncertain of the capability to control its own forces, unable to communicate with its population, or uncertain of the quality of its basic information…"[181] Questions posed by the authors in 1996 for future study (some of which are still undergoing examination today by lawyers) include:

---

177 Ibid.

178 Ibid.

179 Richard Hayes and Gary Wheatley, "Information Warfare and Deterrence," *Strategic Forum*, Number 87, October 1996 as downloaded from Phil Taylor's Web Site, University of Leeds, UK, at http://ics.leeds.ac.uk.

180 Ibid.

181 Ibid.

- What is an information attack? When is it an act of war?
- How is an information attack verified? How is the attacker confirmed?
- Does system penetration equate to an attack? What is an IW version of hostile intent?
- Are there potential tripwires? Who should respond and how for the US?[182]

Two years later, in 1998, Professor Roger Barnett, while teaching IW and arms control at the Naval War College, wrote on information operations, deterrence, and the use of force for the *Naval War College Review*. He wrote that "general" deterrence can work through the denial of an opponent's ability to carry out an attack. It must be backed by an offensive capability with the will to impose punishment on an aggressor. "Focused" deterrence, on the other hand, represents a nation's effort to dissuade an adversary from carrying out an undesirable act. It works best against organized groups, whereas general deterrence works best against less formal groups—computer hackers or terrorists—where deterrence by denial is more appropriate. Information operations in the US rely on general deterrence where, in Barnett's opinion, the US capability to deny is suspect and its will to punish somewhat questionable.[183]

In recent years some of the US's most important IW theorists have focused their attention on a more narrow aspect of information deterrence, that being cyber deterrence concepts. Several examples come to mind immediately. Some analysts support the concept of cyber deterrence, some do not.

First, an interesting discussion over the future of cyber deterrence took place on the pages of *Armed Forces Journal*. Air Force Colonel Stephen Korns contested Colonel Charles Williamson's statement that botnets are a valid cyber deterrent model. Korns used the case of the Russian-Georgian cyber war in August 2008 to make some of his key arguments. He noted that Georgia's relatively easy counter to Russia's use of botnets indicates that botnets have little deterrent effect. If a side can overcome them, then they do not deter a side from acting. If a nation cannot ensure that its cyber deterrent "will inflict severe and specific costs" then it is not a deterrent.[184] Thus in this case one person supports the concept and one does not.

Second, Ambassador Marc Grossman and retired General Harry Raduege, who served as co-chair of the Center for Strategic and International Studies (CSIS) Commission on Cybersecurity for the 44th Presidency, stated in August 2009 that cyber deterrence must "become a top priority for this new official [referring to the new cyber security coordinator at the White House]."[185] Grossman and Raduege advocated for a cyber-triad to deter information network attacks on the US: resilience, attribution, and offensive capabilities. That is, the US must be able to sustain an attack and have a

182 Ibid.

183 Roger Barnett, "Information Operations, Deterrence, and the Use of Force," *Naval War College Review*, 1998, as downloaded from http://www.au.af.mil/au/awc/awcgate/navy on 4 September 2009.

184 Stephen W. Korns, "Botnets Outmaneuvered," *Armed Forces Journal*, January 2009, p. 38.

185 Marc Grossman and Harry Raduege, "Building Cyber Deterrence," *Defense News*, August 24, 2009, p. 29.

retaliatory system in place, be able to identify who initiated the attack, and be able to launch counterstrikes. Grossman and Raduege concluded their article noting that not only the government but also private industry must buy into this concept for it to be successful, since the two are so interrelated today.[186]

Third, one of the US's preeminent scholars on IW issues, Professor John Arquilla of Naval Postgraduate School, wrote that a way to restrain Russia was to "deploy a US-led or NATO-sponsored cyber deterrent squad to disrupt the Russian military's communication networks…"[187] Arquilla stated that he likes "the idea of cyber deterrence being used against anyone who would start a war"—even, he muses, the US.[188]

Finally, US IW specialist Martin Libicki, one of the original developers of the IW concept, recently wrote a long RAND monograph on the issues of cyber attacks and cyber deterrence. Libicki states that he had "chosen to define cyber deterrence as deterrence in kind to test the proposition that the US, as General Cartwright offered, needs to develop a capability in cyberspace to do unto others what others may want to do unto us."[189] The aim of deterrence is "to create disincentives for starting or carrying out further hostile action."[190] Libicki is against the concept of cyber deterrence, noting that "the ambiguities of cyber deterrence contrast starkly with the clarities of nuclear deterrence."[191] He listed several reasons why the ambiguities of cyber deterrence make the deterrence concept untenable in his opinion:

- Will we know who did it? In the case of cyber attacks, attribution is often guesswork. Mistaken attribution makes new enemies and neutrals can confuse retaliation with aggression.[192]
- Can retaliators hold assets of the attacker at risk? There is no guarantee that attackers in cyberspace will have assets that could be put at risk.[193] Is it reasonable to retaliate against a hacker who has done significant damage to a banking or industry infrastructure? What assets does a hacker possess?
- Can retaliators do so repeatedly? Can a retaliatory attack ensure that an attacker will not attack again? While this was probably the case during a nuclear attack it is far less likely after a cyber attack, when the attacker may close off vulnerabilities.
- Can retaliatory cyber attacks disarm cyber attackers? If the attacker is a hacker who could be anywhere, the answer is probably not.
- Will third parties stay out of the way? Nation-states may stay out of the way but it is uncertain if other elements (non-state actors such as terrorist or criminal groups who want to get in on the action) will do so.

186 Ibid.
187 John Arquilla, "Go on the Cyberoffensive," *Wired*, October 2009, p. 99.
188 Ibid.
189 Martin Libicki, *Cyberdeterrence and Cyberwar*, RAND, 2009, p. 27.
190 Ibid., p. 28.
191 Ibid., p. xvi.
192 Ibid.
193 Ibid., p. xvii.

- Might retaliation send the wrong message? An explicit deterrence policy defining cyber attacks as acts of war may encourage private enterprises to lose their incentive to invest in cyber security, knowing that someone above them (government policy) has a larger incentive to protect their business.
- Can states set thresholds for response? It is difficult to establish a threshold and to prove when it has been crossed and by whom.
- Can escalation be avoided? While retaliation may or may not be "in kind" (another cyber attack), it does not guarantee that a counter-retaliation will also be "in kind." A fight that starts in cyberspace may carry over to other means.[194]

These are all tough, legitimate questions. Another question that might have been proposed is "what is the actual intent of electrons involved in an attack? Were they intended to conduct reconnaissance but were misinterpreted? How would an irrational actor respond to a reconnaissance effort?" If a nuclear weapon was involved, everyone would know about the incident.

Some reviewers of Libicki's work found that it had omissions. Retired Colonel Jeffrey Caton noted that the work had missed how state sovereignty is defined in cyberspace; had compartmentalized military aspects of cyberspace from other instruments of power (diplomatic, economic, information); had not discussed second- and third-order effects; and had oversimplified the assumption that deterrence and war in cyberspace are uniquely ambiguous.[195]

In addition to urging caution against the implementation of a cyber deterrence concept for the reasons mentioned here, Libicki also suggests that the US and the US Air Force "should not make strategic cyber war a priority investment area. Strategic cyber war, by itself, would annoy but not disarm an adversary."[196] Further, if strategic cyber war is not a priority for the US, then why spend money on cyber defense and cyber security? Libicki appears to abandon even the concept of a defensive strategic cyber war policy.

Conclusions: What Does This Mean for the Deterrence Concept?

The discussion above indicates some significant differences exist in the nuclear and information/cyber deterrence concepts. And there are other differences not addressed above. Of primary significance is just the construction, transport, and delivery issue. For nuclear weapons, a host of measures are required for each step of the process. Remaining covert during each step in the process is extremely difficult. The construction, trans-port, and delivery issue is of less concern in the information/cyber concept. In this case, a good algorithm writer with knowledge of an important network's landscape can do much damage and do so surreptitiously.

194 Ibid.

195 Downloaded from http://afri.au.af.mil/review_full.asp?id=167.

196 Libicki, p. xix.

Another difference involves the pain and destruction associated with the attack. The pain that a nuclear explosion imparts is well-known. We can watch videos of blasts and predict destruction and fall-out impacts. The pain of an information/cyber attack is less predictable. In the final analysis, social chaos and psychological fear are the immediate fall-outs that most expect. A cyber attack on a banking system can produce panic overnight. What is less known are the effects of an attack on a digital decision-making apparatus, on an industrial infrastructure in winter in the northern part of America, or on a communications satellite. An attack on underwater cables has already taken place and, while sites were down for weeks, it did not generate the type of panic that a mushroom cloud would produce. Thus, for the immediate future the two types of deterrence cannot be equated, as one absolutely negates the use of the weapon (nuclear) while the other (cyber attacks) occurs daily and to date has not witnessed an attack anywhere near the destruction and impact of the attack on Hiroshima more than sixty years ago.

Nuclear deterrence has a history and there has been ample time to discuss the issue. The advent and development of an information/cyber deterrence history, associated with technology, is much shorter. However, advancements have been extraordinarily fast. In the past fifteen years we have witnessed the development of thumb drives, Facebook, YouTube, and other online progress. Quantum computing is here already as well. These cyber advancements offer new ways to consider deterrence beyond the term's nuclear heritage. For example, the term can be viewed from the perspective of deterring math attacks on data or deterring verbal/image attacks that hamper understanding.

Another difference is that under the umbrella of nuclear deterrence only governments of nation-states played. Under an information/cyber deterrence standoff, anyone can potentially play. No longer are we tied to governments and ambassadors and foreign ministries as the negotiators of nuclear deterrence. The cyber world operates in stark contrast to the nuclear one as extremists and terrorists see opportunities to play on the cyber field, which the nuclear era did not offer.

Information/cyber deterrence must go beyond the historical context of deterrence associated with the nuclear age. It must expand and advance the discussion. An attacked country must be ready to perform deterrence in depth (more MacAfee?), deterrence through punishment (use of a cyber attack against a cyber attack, or use of an international legal mechanism against a cyber attacker), or deterrence through a threat to a comparable value within the country of an attacker. People should use the shell of nuclear deterrence as background on deterrence issues, but with the information/cyber concept more issues are at stake and they invite a more flexible look at the deterrence concept. The concepts of persuasion, extortion, defense in depth, preemption, and flexible response have different applications and different results when used with information/cyber issues than with nuclear destruction. With nuclear weapons we knew who the enemy was. With information/cyber issues, we do not always know. In short, it is time to talk about what we really mean by information deterrence separate from the nuclear heritage of the term "deterrence." The information/cyber age has

distinctive characteristics that we must work with in the future.

Another issue involves the legal aspect of nuclear versus information/cyber deterrence. Entire treaties and policies have already been developed to contain the spread and use of nuclear weapons. The construction of a similar system for information/cyber deterrence issues remains far off in the future. The issue is still too uncertain for a final policy statement, as nations fear being contained by issues they could not foresee based on a lack of practical experience in the area.

China appears to have developed an understanding of cyber deterrence that is a combination of the influence of traditional thought and lessons learned from watching the West, in particular the US. On the one hand, there are the key factors in Sun Tzu's writings that influence contemporary deterrence theory. These include having superior military power, being fully prepared for war, having severe measures of punishment at one's disposal, having superb skill at "attacking strategy" and "attacking diplomacy," and making one's ideology of deterrence a linchpin in a more complete system.

The essence of China's deterrence practice is to resolve war with non-war measures and to apply stratagems such as win without fighting and win victory before the first battle. To win with stratagems, the Chinese must prepare a counter-deterrent to US actions. This might involve mimicking US policy moves with near mirror-image moves of their own; using military exercises to demonstrate strength in the use of technologies; and perhaps using their massive computer reconnaissance activities to uncover frequencies and other operating parameters of US systems. Such activities can be turned into reliable counter-deterrents to US cyber capabilities.

The myriad of problems associated with cyber deterrence indicates that this is an area of continuing discussion if states are to intelligently thwart or simply confront future information/cyber crises. It is time to think hard about these problems and develop some potential solutions before we are dealing with practice instead of theory. Yogi Berra, the longtime catcher for the New York Yankees in the 1950s and 1960s, who is famous for his malapropisms, issued a proper warning: "in theory there is no difference in theory and practice. In practice, there is." States must be theoretically prepared for such information/cyber crises if they are to offer the best practical response to the crises before them. Thorough discussion of these issues is mandatory on a multilateral basis.

CHAPTER THREE
ENHANCING DETERRENCE THROUGH NEW CYBER ORGANIZATIONS

As information of a country's crucial finances, utilities, satellite and telecommunication facilities, and strategic military installations is now linked by one cable—and theoretically accessible to top-notch hackers—it is important for a sovereign nation to erect the best possible firewalls to deny others' attacks. And, in time of conflict, the ability to launch a counterattack to disable the enemy's operations is also indispensable.[197]

Introduction

During the period 2009-2011, Chinese open source military writers and policy officials unveiled several new cyber-related developments,[198] which helped generate combat power to a higher degree and thereby enhance deterrence and the combat capabilities of the military. New equipment, organizations, and ideas included a supercomputer, a new cyber center, new online military games (some designating the US as the opponent), a name change of a general staff department (from "communications" to "information technology"), the development of a cyber blue army (to serve as an opposing force for the People's Liberation Army's [PLA] cyber red force), and several other information-related developments. Information-related modifications across the board have resulted in a situation where one plus one is greater than two for the effectiveness of military power.

What follows is a description of each development. The result is an evolving mosaic of China's cyber intent and future plans whose goal is to transform the nation into a strong US cyber competitor and to use that strength as a deterrent toward US policies and plans.

New Developments, Organizations, Online Games, Units

The first and perhaps most important development came in November of 2011 when the Chinese announced the unveiling of the world's most powerful supercomputer, the Tianhe-1A. The supercomputer, also called the Milky Way according to *Newsweek*, can reportedly conduct 2.5 quadrillion operations per second. The US Livermore Lab's best supercomputer, the Blue Gene/L, can perform .5 quadrillion operations per second. Supercomputers help design weapon systems, model climate change, crack

197 Li Hong, "China's Cyber Squad is for Defense," *Renmin Ribao* (in English) 31 May 2011.

198 In the Chinese book *The Science of Military Strategy*, the authors (two influential PLA generals) provided an appendix of terms. The book was translated into English by the Chinese. They noted that the Chinese character for cyber was identical to the character for informationization. For this reason, cyber is used often in place of informationization in this chapter.

codes, develop new drugs, and enable countries to compete in not only science but also in industries like oil and gas exploration.[199] One US computer scientist feels that in five years China will "have their cyber-infrastructure connected. They could create a distributed supercomputer that is 100 times faster than anything we have in the US."[200]

Actually, the Chinese and other nations had been discussing the Tianhe-1A for nearly a year before the *Newsweek* article appeared. A Taiwanese report in March 2011 noted that the Tianhe-1A had taken "the top spot in the Top 500 list of the world's most powerful supercomputers last November…"[201] Further, one seventh of the systems central processing units (CPUs) are China-made for the first time. Currently the majority of the CPUs used in the Tianhe-1A are made in the US. It is believed the supercomputer will be used to develop nuclear fusion energy, to conduct molecular dynamic simulations, and to aid in climatic studies. The supercomputer has also been heralded by scientists working on seismic issues, meteorology, medicine, commercial design, and construction. One source noted that the processor can compute 1.87 petaflops per second.[202]

Livermore Labs is busy designing a new supercomputer that reportedly will have eight times the computing power of the Tianhe-1 A, or 20 quadrillion operations per second. The computer, named Sequoia, is to be finished by the end of 2012. A decade beyond Sequoia, Livermore is planning to develop an "exascale computer" which reportedly can deliver 500 times the computing power of Sequoia.[203] An exascale computer is designed to compute beyond the current petascale and could, according to a Chinese source, represent a thousandfold increase on that scale. China's 2015 goal is to create a computer with a "100 petaflops a second" capacity in preparation for the development of an exascale computer in 2020 or two years before a US model would appear.[204]

On 19 January 2012, China's *Xinhua News Agency* announced the development of the Chinese Sunway BlueLight Supercomputer in Jinan. It can reportedly perform one thousand trillion calculations per second. One US consultant to Los Alamos National Laboratory stated that the most impressive part of the supercomputer was its homegrown nature, with most of the microprocessors coming from China. *Xinhua* notes that the computer will be used in oceanography, biopharmacy, industrial design, and financial risk prediction. It will also serve as a node in China's national computing grid.[205]

The second major cyber development, this time involving the PLA, is the creation of a cyber center and an information department in the general staff of the PLA. Both

199 Dan Lyons, "Be Afraid. Be Very Afraid," *Newsweek*, 5 December 2011, p. 58.

200 Ibid., p. 59.

201 Cheng Hui-yuan, "Made in China Processors Power World's Fastest Supercomputer," Taipei's *Want China Times* (in English), 25 March 2011.

202 Mao Zhenhua, (no title), *Xinhua Domestic Service*, 11 June 2011.

203 Lyons.

204 Unattributed article, "Race Is on for New Generation of Supercomputer Industries," *China Daily* Online (in English), 20 August 2011.

205 Zhang Yunlong and Zhou Zhou, "China's Sunway BlueLight Supercomputer Goes into Operation," *Xinhua*, 19 January 2012.

represent major developments. In 2010 the Chinese announced the creation of a cyber-based headquarters or center responsible for tackling potential cyber threats and safeguarding national security. A general staff officer stated that "the base just means that our army is strengthening its capacity and is developing potential military officers to track information-based warfare."[206] He stated the base would be used "to gather online information" [author: is he referring to just website information or to invasive reconnaissance?] and build up walls to safeguard information. Finally, he stated that "it is a defensive base for information security, not an offensive headquarters for cyber war."[207] The development of an informatization department in the general staff was created on 30 June 2011 but was not announced until early July. A *China Daily* report noted that the Communication Department of the General Staff was to be restructured and renamed the Informatization Department. The announcement mentioned that this was a new step toward developing further the requirements for an information-based PLA and would affect communication units at corps level and above.[208] Another source, *Xinhua News Agency*, called the new department the Information Technology (IT) Department and stated that it was developed based on a strategic perspective.[209]

A third major development, also PLA related, was Chen Weizhan's announcement in 2011 that China had used an "Online Blue Army" in a training exercise, the first time such an announcement had been officially made. It was noted that:

> An 'online Blue Force' held online confrontations concurrently with four 'Red Forces' and ended up scoring a military success of 'three wins and one loss.' In the latter part of April the Guanzhou Military Region organized an online off-site concurrent exercise in which the 'online Blue Force' hit out in all directions, changing the previous 'one-on-one' confrontation model and calmly using network-based new operational methods on a 'one-on-many' intangible battlefield to make online confrontations more exciting and fiercer.[210]

It is unknown whether there is a link between the 2010 cyber center and the Cyber Blue Force.

Outside observers of this announcement immediately recognized the implication that China has the offensive capability to attack four digital units at once. Or, the implication could be that the Red Force is very vulnerable to cyber attacks. The Blue Army used viral attacks, garbage messages, and infiltration and penetration methods

206 Peng Pu, "PLA Unveils Nations First Cyber Center," *Global Times* Online (in English), 22 July 2010.

207 Ibid.

208 Zhang Yanzhong and Li Qiang, "GSH Communication Department Restructured into an Informatization Department," *Jiefangjun Bao* Online (in English), 1 July 2011.

209 "PLA General Staff Headquarters Establishes IT Department," *Xinhua* (in English), 1 July 2011.

210 Lei Ming and Yan Deyong, "Mighty Force Locked in Fierce Contest on Intangible Battlefield," *Jiefangjun Bao* Online, 17 May 2011, p. 1.

of internal networks according to the report. Digital reserve forces used many of these same techniques several years ago, implying that the Blue Force activity was not as new as the admission that such a force existed.

China may be attempting to fold the Blue Force into the PLA's active defensive theory. They have stated, for example, that the Blue Force is a network defense training mechanism for the Red Force. The same article describes the Blue Force as a way to enhance transparency and a way to extend its strategy of deterrence.[211] The latter claim, along with the offensive character of its Blue versus Red force exercise, indicates that the PLA has a strong offensive capability that cannot go unnoticed! Other writers have stated that the Cyber Blue Force is different from hackers in that it is legitimate. It was set up by a department of the state. The PLA hopes that the concept will help uncover and erase many of its problems with cyber concepts, as well as improving the functions, mission, facilities, and regulations of the cyber army. International legislation associated with cyber issues also needs improvement.[212] More information on the Online Blue Army is contained in Chapter Eight.

A fourth development was the creation of several information-related departments in the PLA's regions and academies. It is expected that the military regions will change their communication departments to informa-tization departments or units in line with the announcement by higher headquarters. The overall goal of the renaming process most likely is to prepare the force to fight local wars under informatized conditions. The move also seems designed to support the PLA's organizational focus on improving its system-of-systems (SoS) operational capabilities and its management and support systems. In a related issue tied to the operating principles of the Informatization Department, a military observer in Guangzhou wrote that the PLA relies on its own Intranet and optical fiber, telephone, and wired radio networks to stay safe from cyber attacks.[213]

Several other cyber or information-related departments were formed across the PLA. It was reported that the National University of Defense Technology established an Information Technology Department.[214] The PLA established an Information Logistics Support Base of the General Staff Department in July 2011, the first strategic information service arm of the PLA. The Communication and Command Academy was reorganized as the National Defense Information Academy. These steps, along with the other efforts, are designed to intensify the scientific development and consolidation of the PLA's informationization process. They also serve to improve the PLA's training efforts in an "environment of extensive informationization."[215] The investment into

211 Ni Erh-yen, "Put Aside Weapons to Really Show Your Military Skill: PLA's Creation of 'Net Blue Force' Conveys Positive News," *Wen Wei Po* Online, 4 June 2011.

212 Guo Lei, Gu Caiyu, and Wu Nan, "Why Has China Established a Cyber Blue Army?" *Renmin Ribao* Online, 27 June 2011, p. 1.

213 Yao Yijiang, no title listed, *Nanfang Zhoumo*, 14 July 2011.

214 No author, "Beijing News from the Grapevine: PLA Unwilling to be 'Supporting Actor' and Therefore Makes a Move," *Ming Pao* Online, 2 December 2011.

215 Ma Hao-Liang, "'Beijing Observation' Column: Transformation in PLA Planning Reflects Hu Jintao's Strategy for Building the Military," *Ta Kung Pao* Online, 24 November 2011.

informatization has been the most noteworthy aspect of military reform so far. The PLA believes that warfare is now so focused on cyber warfare and the electromagnetic spectrum that the reform focus in this area is justified. Improvements have been felt in areas such as "strategic information warfare, command and control, training, support and logistics provision, personnel development, and so on."[216]

The essence of this military reform effort is a top-down redesign process that was underscored with the establishment of a Strategic Planning Division to control the process. Here, the mission is to

> Formulate strategic schemes, because only if the strategic objectives are clearly identified in advance and the approach for strategy implementation is well considered will the various key departments, the major military regions, and the different arms of services be able to purposefully and progressively build up their efforts in military reconstruction under the general strategic framework.[217]

The establishment of a Strategic Planning Department signifies a serious PLA effort to envelop traditional and cyber-related war fighting capabilities, plans, and policies into a united effort. The department is designed to serve as a key think tank for the Central Military commission; to coordinate the strategic planning of the armed forces, optimizing their allocation, distribution, and integration; and to look ten steps ahead to eliminate blind or random decision-making. This helps the PLA to win a war before it starts. The department meets the needs of facing systemic operations and information warfare challenges.[218] The department "will also help with coordinating informatized, interactive command among the different departments and services of the PLA,"[219] and will help develop the stages for the PLA to follow as it proceeds from mechanization to meet the requirements of informatization.[220] Another source offered that the department has geopolitical issues to address, stating that the department was created due to US pressure in the region, especially in the "four seas" (Yellow Sea, East Sea, Straits of Taiwan, and the South China Sea) area where China feels "the image of the US and its allies."[221]

There are several non-PLA related cyber security organizations in China. These include the Ministry of Industry and Information Technology (MIIT, which has a mission for information security); the National Computer Network Emergency

216 Ibid.

217 Ibid.

218 Luo Yuan, "Setting Up the PLA Strategic Planning Department is a Move Up the Strategic High Ground," *Zhongguo Qingnian Bao* Online, 2 December 2011.

219 Li Qianting and Wang Xiaoxue, "Military's Establishment of New Department is Not Aimed Solely at the Disputes in the South China Sea," *Wen Wei Po* Online, 28 November 2011.

220 Guo Yuandan, "PLA Sets Up Four New Departments in One Month—Expert," *Fazhi Wanbao* Online, 22 December 2011.

221 Xue Litai, "Beijing Feels Intense Challenges Both Internal and External, Sees Need to Upgrade Strategic Planning Department to Counter Washington," *Lianhe Zaobao* Online, 25 November 2011.

Response Technical Team (which focuses on security for public networks); the China Association of Communication Enterprises and Cyber Security Specialists Committee; the China Information Technology Security Evaluation Center; and the National Computer Virus Emergency Response Center.[222] Other administrative elements include the General Administration of Press and Publication (GAAP), the Ministry of Culture, the State Administration of Radio, Film, and Television, and the Ministry of Public Security (responsible for cybercrime among other issues).

In May 2011 China announced the approval of a State Internet Information Office. The new office's duties reportedly include implementing an Internet information dissemination policy and working closely with other government agencies in strengthening the oversight of online content. Further, it is charged with monitoring telecommunications operators, Internet service providers, domain registrars and hosting providers, IP address allocation, website licensing and registration, Internet access, and other infrastructure-level operations. The office is based in the State Council Information Office, the government's propaganda and information arm. Wang Chen will be the director of both agencies.[223] China's *Digital Times* offered a slightly different version of the office's duties. It noted the following:

- The department will direct, coordinate, and supervise online content management and handle administrative approval of businesses related to online news reporting.
- It will direct the development of online gaming, online video, and online publication industries.
- The office will be engaged in promoting construction of major news websites and managing government online publicity work.
- It is assigned the duties to investigate and punish websites violating laws and regulations.
- It will oversee telecom service providers in their efforts to improve the management of the registration of domain names, distribution of IP addresses, registration of websites, and Internet access.[224]

Thus the duties of the new office are focused on management and enforcement duties.

A fifth development was the release of computer war games for PLA soldiers. The most prominent of these was the "Glorious Mission" game that the Nanjing Military Region developed. It was reported that the region's command and the Wuxi Giant Network Technology Company, Limited, worked jointly on the project. Thirty-two soldiers can reportedly log on at the same time in squad/team confrontations, according

222 Information provided to the author by Chinese expert Alastair Iain Johnston, Harvard University, on 28 January 2011.

223 Francis Tan, "China Sugarcoats 'Big Brother' as State Internet Information Office," *The Next Web*, 5 May 2011 located at http://thenextweb.com/asia/2011/05/05.

224 "China Sets Up State Internet Information Office," http://chinadigitaltimes.net/2011/05/china-sets-up-state-internet-information-office/

to the rules.[225]

The game has three modules—basic training, individual soldier missions, and team-to-team confrontations. The game offers soldiers a chance to experience a "tense political atmosphere and exciting barracks life, but also gives them a chance to acquire knowledge, temper their courage, widen their knowledge base, and develop outstanding political character, fighting spirit, and mental toughness."[226]

Online games are designed for "innovating and developing an advanced military culture and enriching officers' and soldiers' spiritual and cultural life."[227] The games are developed by Chinese software makers, contain genuine PLA characteristics, and utilize advanced technology so that lifelike astronomical and weather conditions can be used.[228] The Second Artillery Force proudly acclaimed that its game developers had created ten kinds of software, covering military development, virtual training, combat, leisure and puzzle games, and, most important for this discussion, offensive and defensive Internet strategies.[229]

New Computing and Cyber War Model Developments

In addition to new organizations and units, the PLA's cyber progress was noted in the development of computer prowess and theoretical accomplishments. Some of these developments were in software, quantum computing, and cyber modeling.

A few years ago the Nanjing Military Region undertook an effort to improve its software writing capability. It was noted that hardware without software is like having a beautiful box without a pearl inside. Several steps ensued to improve software. The region's commanders took advantage of the software industries in East China, took the Military Region's command automation work stations as the principal actors, actively cooperated with large-scale software enterprises and scientific research institutes to research and develop military software, and raised the standard for military software construction. The region thus developed a "military software park." A major goal of the project was to fix software incompatibility and to ensure that future software projects would be compatible. The software park has already yielded results, enhancing unified research and development as well as software sharing and standardization. Another issue was to help with software maintenance after installation.[230]

China reports that its quantum computing capability is now beginning to show improvement. For example, in the journal *New Scientist*, author Gregory Huang described the dreams and aspirations of the Chinese to quickly develop a quantum computing device. In an interview with Pan Jian-Wei of the University of Science and Technology (UST) of China, Huang described how Pan is trying to combine "quantum

225 Wang Dongpin and Liu Gang, "Glorious Mission Fills in Blanks in Computer Military Game," *Jiefangjun Bao* Online, 13 May 2011.

226 Wang Dongpin and Xiao Jinbo, "'Glorious Mission'—First Large Military-Themed Computer Game Rolled Out in China," *Renmin Ribao* Online, 27 June 2011.

227 Ibid.

228 Ibid.

229 Cai Ruijin and Zhang Qi, "SAF Completes Development of Military Electronic Games," *Jiefangjun Bao* Online, English, 18 July 2011.

230 Ouyang Hao, Li Dingjiang, and Fang Fei, "Buy the Box to 'Look for' Pearls': Building 'Military Software,'" *Jiefangjun Bao* Online, 18 March 2011, p. 2.

memory with a new architecture known as cluster states."[231] Quantum computing inspires researchers to use quantum mechanics to perform tasks that current computers cannot. As Huang explains

> The power of a quantum computer comes from the fact that a quantum particle can exist in more than one state at a time. So unlike a data bit in an ordinary computer, which can have the value of either 0 or 1, a quantum bit (or qubit) can simultaneously have the value 0, 1, or any "superposition" of the two. So perform a calculation using qubits and you get a huge number of calculations for the price of one.[232]

When the quantum theory known as entanglement is added to the quantum phenomenon, Huang notes, it can link the properties of several qubits. Then, in principle, it is possible to represent more numbers than there are atoms in the universe.[233] Problems do exist, however. In this case the problem is the stability of an "entanglement." It turns out they are very fragile. "Cluster states," where each step has its own calculation, is Pan's attempt to overcome this problem and maintain stability with the use of photons for quantum communication. No entanglement manipulations are necessary, as they are prepared and left alone. This does, however, require preparing more entanglements before the calculations start.[234] China's progress indicates that scientists are moving quickly forward and making strides in many technical areas to which new thinking (or the application of old stratagems) can be applied.

In August 2010, an *Asia Times* Online article further discussed the concept. Researchers at Tsinghua University and the Hefei National Laboratory for Physical Sciences reported that they had demonstrated a quantum teleportation of over sixteen kilometers of free space. Instead of transporting matter from place to place, the current application transports photons, ensuring almost totally secure data communications. It works as follows: after two particles get linked, the state of the particle at the sender's end is destroyed and reappears as an exact replica at the receiver's end, with a super small chance of undetected third-party interception. The blue lasers used in the technology appear to penetrate further into water and thus have wider applicability for subsurface communications than current US infrared lasers. According to the report, a satellite-based quantum laser system would offer the military a secure means of communication.[235]

With regard to a cyber warfare combat model, a *Zhongguo Qingnian Bao* Online report by two authors from China's National Defense University stated that network war is really composed of five operational forms: intelligence, paralysis, defense, psychology, and network-electromagnetic integration (or INEW, integrated network-electronic warfare). Network intelligence is described as large in quantity, of high

231 Gregory Huang, "Master of Qubits," *New Scientist*, 10 November 2007, p. 69.

232 Ibid.

233 Ibid.

234 Ibid., p. 70.

235 Matthew Luce, "China's Quantum Secure Communications," *Asia Times* Online (in English), 26 August 2010.

classification, timely, and of low cost. Further, the authors note that "reconnaissance activities that are launched over the Internet are already omnipresent and are extremely difficult to defend against."[236] Paralysis warfare is really attack warfare. It uses attacks on nodes and trunks to induce maximum results with minimum efforts. Network defense includes security assessments, monitoring and warning, defense against intrusion, and emergency recovery. Active defense is combined with deep defense. [237]

Network psychological operations consist of a multi-element arena that combines cell phones, blogging, podcasting, and other functions with the goal of influencing public opinion. The PLA authors offered the following development of events that touch on the network-psychological operations concept:

> A street vender lights himself on fire, WikiLeaks reveals that the president is corrupt, social public opinion ferments, popular sentiment on network 'socializing platforms' expands, the people go out into the streets, the security situation spirals out of control, things spill over into neighboring counties, major Western powers get involved, the domino effect kicks in, and Libya finds itself under the sword.[238]

INEW consists of signal-level energy suppression, network-level protocol attacks, information-level deception, and so on.[239]

Some Chinese activities appear to fit a few of these categories. For example, a Chinese report of June 2011 stated that the US Senate complained loudly about substandard computer chips from China becoming components of advanced US weapon systems. Senate Armed Services Committee Chairman Carl Levin stated that counterfeit electronics had infiltrated the Pentagon's supply chain. The committee's investigation "almost totally and exclusively" pointed to China and specifically to Shenzhen as the source of the parts. Zhang Zhaozhong, a PLA professor at China's National Defense University, blamed the US for failing in its procurement inspections. Song Xiaojun, another Chinese military expert, stated that the purpose of citing inferior products was to derail a proposed military budget cut.[240] So this episode could be classified as an intelligence activity to plant viruses or as an attack or paralysis activity that is designed to render US equipment unusable.

In July 2011 the PLA held a class on advanced-level techniques for network offensive-defensive operations. Cadres from PLA science and technology research institutes took part in the class under the sponsorship of the General Political Department. Both military and civilian experts gave lectures.[241]

---

236 Ye Zheng and Zhao Baoxian, "How Do You Fight a Network War?" *Zhongguo Qingnian Bao* Online, 3 June 2011.

237 Ibid.

238 Ibid.

239 Ibid.

240 Li Qian, "'Fake Chips' Cause Fury in US Senate," *Global Times* Online (in English), 16 June 2011.

241 Chan Shigang and Chi Weizheng, "PLA Holds Classes to Teach Cutting-Edge Network Offense-Defense Information Confrontation Techniques," *Keji Ribao* Online, 19 July 2011.

Finally, there were several older topics that continued into 2010 and 2011, such as the focus on information-based SoS theory, planning, and operations. Identifying key components of another force's operating systems continued to draw attention; and continuing calls were made for the use of asymmetric operations to create situations where weaknesses could be changed into strengths. Such operations focused on striking logistical support systems, identifying cyber vulnerabilities in opposing forces, and renewing combat theories in light of informatized warfare developments.[242]

Continued Emphasis on Mobilization and People's War Concepts

China's national defense mobilization planning strives to rapidly integrate peacetime-wartime capabilities and to tie together front and support activities. The ultimate goal of planning for informatized mobilization operations is to utilize the SoS concept. This is to be accomplished through precisely mobilizing, organizing, computing, controlling, implanting, and evaluating combat operational demands.[243]

Informatized mobilization is defined as precise combat operations in which various combat forces, combat elements, and combat actions realize seamless linkups at different times in space via informatized means and platforms.[244] In order to meet the undetermined requirements of future battlefields, the PLA must be able to respond to a variety of threats and accomplish diversified military tasks. Further, this requires that militia and reserve specialized detachments be optimized. The overall mission of the mobilization system, once complete, is to do the following:

> Raise the capability to provide specialized support in information-system based system-of-systems operations; and the information offensive and defensive detachments have to focus on information scouting, information jamming, and information offensive and defensive training and on 'three warfares' training, with emphasis on raising the information offensive and defensive capability in information system-based system-of-systems operations.[245]

In spite of advancements in the mobilization capability of the country, the PLA still faces problems. First is that the mobilization of national defense means is a government responsibility that currently is military-led which places the armed forces in charge of implementation. A complimentary civilian-led mobilization has still not materialized causing the civilian sector to lag behind the military in this regard. Second, there remains a fuzzy overlap of responsibilities. Third, China is working from an outdated reporting mechanism. There is no clear set of instructions on how to handle requests or report military demands in peacetime or wartime. Finally, China's laws and regulations still appear inadequate and lacking in a concrete legal basis for establishing, staffing,

242 Zhang Hui and Liu Yong, "Think More of Asymmetric Operations," *Zhongguo Guofang Bao* Online, 16 May 2011, p. 3.

243 Chang Yeting, "Accelerate Transformation of National Defense Mobilization Capability Generation Model Surrounding Demands of Information System-Based System-of-Systems Operations," *Guofang*, No. 8 2011, pp. 30-33.

244 Ibid.

245 Ibid.

and assigning duties of the mobilization command. The further integration of military preparations with local economic and social capabilities must also be completed.[246]

Mobilization of all resources, combined with the integration of military and civilian capabilities, leads directly to discussions in China of continuing the concept of People's War, albeit under contemporary conditions of informatized warfare. People's War implies the entire nation rising up to confront an aggressor. In the digital age this indicates the integration of mobilization capabilities and the civilian use of information-age developments (hacker tools, etc.) that enable every citizen with a laptop to fight against an enemy, even from thousands of miles away. People's War is also used by the Communist Party of China (CPC) to keep the military under its control. For example, a *Zhongguo Guofang Bao* Online report of 22 August 2011 noted that not only is People's War a magic weapon for winning an informatized war that involves both the armed forces and civilians, but also a concept in which the PLA's forces should uphold their People's War thinking. Leaders should bring into play the superiority of China's armed forces that are placed under the leadership of the CPC organizations of corresponding levels.[247]

In People's War under informatized conditions, what is important is the technological competency of personnel more so than their quantity. The Internet has broadened warfare's competency far beyond the battlefield. Now warfare can include economic and even cultural components in addition to network warfare. Such warfare means further calls for more precision in warfare than was postulated during traditional warfare.

Such explanations imply that People's War in the future will have two elements: first, the ability to fight with traditional warfare means (artillery, tanks, infantry) under high-technology conditions; and second, fighting informatized warfare against adversaries who are trying to disrupt or destroy electromagnetic, satellite or space weapons. Masses of people may still be used in warfare but with different roles.

An article on People's War under informatized conditions appeared in *China Military Science* in 2009. It underscored the enduring legacy and new conditions under which the concept is viewed. The primary points are that high tech advancements enable military and civilian members of society to participate in the war effort in multiple ways; and that under informatized conditions it is necessary to solicit the full support of the masses for the war effort. To obtain the full support of the masses involves the use of grand strategic thinking and the use of media, legal, psychological, financial, military, political, cultural, and trade warfare forms, among others. Support from the masses can equate People's War with total war. Attempts to seize the initiative and increase the nation's comprehensive strength and war-fighting capability can be indirect or direct. Since warfare will be quick and abrupt, People's War capabilities under informatized conditions must be formed in peacetime and represent the "orderly accumulation" of the total capacity of the state, its armed forces, and the unarmed masses. This requires the creation of new theories in the following four areas: digitized and information

246 Ibid.

247 Sheng Qiang, "It is Even More Necessary to Bring Into Play the Superiority of People's War in Informatized War," *Zhongguo Guofang Bao* Online, 22 August 2011, p. 3.

networks; offensive and defensive methods of operation; education and training; and comprehensive support.[248]

Articles on the topic of People's War under informatized conditions that were footnoted or cited in the 2009 *China Military Science* article included the following works. They demonstrate the continued interest in the topic and its applicability in digital times:

- Meet the Needs in Winning Future Wars, Enhancing the Construction of Informatized Battlefields for People's War (2003)
- Innovate Methods of Operation of People's War According to the Change in the Forms of War (2004)
- Challenges Facing People's War in Informatized Warfare and Thoughts on Countermeasures (2005)
- Interpret People's War under Informatized Conditions (2005)
- New Thoughts about People's War under Informatized Conditions (2005)
- Thoughts on the Challenges in Carrying Out People's War under Informatized Warfare and Countermeasures
- Enhance the Overall Power of People's War under Informa-tized Conditions (2006)
- Innovate and Develop the Strategy and Tactics of People's War (2007)
- Thoughts on Innovating and Developing People's War under Informatized Conditions (2007)
- Tentative Analysis of Views on Winning Victory of People's War under Informatized Conditions (2007)
- New Interpretation of the Thought of People's War (2007)
- Thinking on Maintaining and Developing the Thought of People's War under Informatized Conditions (date unknown)
- Measures and Thoughts on Adhering to and Developing the Thought of People's War under Informatized Conditions (date unknown)
- Enhance the Overall Power of People's War under Inform-atized Conditions (date unknown)[249]

Chinese Thoughts on New US Cyber Strategies

The Chinese analysis of US cyber-strategy-related documents has produced a series of new articles that have warned of dangerous consequences from recent US cyber policies. What has not changed is that the Chinese continue to accuse the US of "hegemonic" plans in cyberspace.

What the Chinese generally ignore in these discussions is that perhaps the US has done China and the rest of the world a favor by openly sharing its perceived threats from cyberspace and the direction and intent of US responses. The US clearly feels it is

248 Wang Wei and Yang Zhen, "Recent Developments in the Study of the Idea of People's War under Informatized Conditions," *China Military Science*, No. 2 2009, pp. 145-151.

249 Ibid.

better to issue a warning and inform other countries (especially China, whose intrusive cyber activities have drawn accusations from numerous states) of the consequences of their actions. Rather than attack without warning the US has issued numerous warnings about the consequences of further hacking activities. Naturally, the Chinese articles on US policy did not take any blame for the fact that their cyber activities helped spawn the US cyber strategy in the first place.

The key cyber documents repeatedly brought up in the Chinese press are the following: Deputy Defense Secretary William J. Lynn's 15 February 2011 discussion of cyber's five pillars; White House Cyber Security Coordinator Howard Schmitt's 16 May 2011 announcement of an *International Strategy for Cyberspace*; and Deputy Defense Secretary William Lynn's 14 July 2011 announcement of a *Strategy for Operating in Cyberspace*.

Several Chinese writers examined Howard Schmitt's international strategy document. Some viewed the strategy as a new arrow in America's deterrence strategy quiver and as a way to maintain its lead in the military sphere. One Chinese article noted that the US developed the strategy in response to Russian and Chinese cyber attacks. Li Shuisheng, a researcher at China's Academy of Military Science, labeled this comment as "baseless conjecture and slander."[250] Fang Binxing, the architect of China's Golden Shield Project (which includes Internet censorship and surveillance projects as part of China's 'Great Firewall'), stated that blaming China for cyber attacks against the US could be an excuse for launching military strikes against China.[251]

A *Xinhua* news article explained how other Chinese analysts interpreted Schmitt's cyber strategy. The authors note that the US thinks cyberspace is a new battlefield where the US can implement deterrence via three channels: the mere possession of cyber weapons, the formulation of cyber weapons research and development plans, and the development of regulations for the use of cyber weapons based on Cold War deterrence theory.[252] The *Xinhua* article added that former US counterintelligence chief Joel Brenner highlighted Russia, China, and Iran as the greatest cyber threats to the US; and that Google again (as it had in January 2010) had accused China of attempting to break into its accounts. Such accusations enable the US to find excuses and imaginary enemies, the Chinese authors stated. They accused the US and Google of "tacit cooperation" in playing up the Chinese hacker threat; and accused Google of "irresponsible" conduct, since it did not provide any evidence that China initiated the attack. The article concluded with the thoughts that the US policy could undermine international mutual trust in cyberspace, that US cyber weapons my hurt the innocent since it cannot be sure who is attacking the US, and that the US could trigger a confrontation between different countries in cyberspace.[253]

---

250 Ren Qinqin, Ren Liyig, and Wang Jianhua, "US Defense Department's First Cyber Strategy May Bring Dangerous Consequences," *Xinhua Asia-Pacific Service*, 1 June 2011.

251 Stephen Cheng, "Beijing Hits at Pentagon's Cyber Strategy," *South China Morning Post* Online (in English)," 3 June 2011.

252 Zhang Xiaojun, with assistance from Ren Haijun, Lan Jianzhong, Yang Lei, Lin Xiaochun, Qian Zheng, Li Wen, and Ren Liying, "Smoke of Gunpowder Looms in Cyberspace as the United States Keeps 'Making Moves'," *Xinhua Domestic Service* Online, 18 June 2011.

253 Ibid.

A *Jiefangjun Bao* Online article in June 2011 emphasized that the outside world views the US cyber strategy as a new excuse for the US military to use force abroad. The US strategy is dual-hatted in that it uses "cyber freedom" to supplement its global diplomacy and "cyber security" to suppress competitors. It wants other nations to open their Internet gates while the US seeks to close its own under the logic of national security. The article also states that General Keith Alexander, US Cyber Command Commander, believes the command should have an offensive capability and a preemptive strike strategy.[254]

Li Daguang, writing as well for *Jiefangjun Bao* Online on 16 June, noted that the US wants to formulate cyber war's rules all by itself in order to control the commanding point of cyber war. With its announcement that it considers cyber attacks as acts of war, the US believes it can use all means—diplomatic, information technology, military, and economic—to respond to cyber attacks. Particularly worrying, according to Li, is the US development of space router technology, a key technology. Putting Internet protocol routers in geosynchronous satellites extends Internet capabilities to space and eliminates many ground-based technological problems. In response, China must intensify its cyber defense construction capabilities, quicken the pace of development of the PLA's cyber strength, and raise its capability for conducting cyber operations.[255]

Xinhua Domestic Service Online carried the commentary of staff reporters Zhang Xiaojun and Li Wen in a final June article on Schmitt's *International Strategy for Cyberspace*. The reporters stated that "it is not difficult to see that the US is developing Internet tools with the intent of undermining other countries' Internet controls and using this as its weapon to support political opponents in other countries."[256] To the reporters, this is a new type of military deterrence that is supported by hard power.[257]

Some articles were less threatening. *Zhongguo Qingnian Bao* Online, for example, wrote on 23 June that the international strategy was a call for both cooperation and confrontation. Pan Zhuting, an executive strategy manager for Beijing's Venustech Incorporated, stated that a cooperation element of the strategy was the proposition that the benefits of networks should serve everyone and not just a few nations. Pan saw potential confrontation with the US over the strategy's phrase that a cyber attack on the US could result in a counterattack with military force. Pan recommended developing a multi-stem-line organization involving multiparty participation.[258]

Other groups differed in how they understood the strategy. Dr. Jiang Jianchun, identified as a member of the Chinese Academy of Science's (CAS) Institute of Software (he once headed a cyber offensive and defensive research group at CAS's Information Security Project Research Center), stated that government, enterprises, and the civilian sector should develop a countermeasure policy together. Harmonious development is

254 Lu Desheng, "US Military Looking for a New Excuse to Use Force Abroad…," *Jiefangjun Bao* Online, 8 June 2011, p. 4.

255 Li Daguang, "Behind 'Upgrading' of US Military's Cyber Warfare Concept," *Jiefangjun Bao* Online, 16 June 2011, p. 12.

256 Zhang Xiaojun and Li Wen, "Do Not Make the Internet a Battlefield," *Xinhua Domestic Service* Online, 18 June 2011.

257 Ibid.

258 Li Xinling, "Is the US 'International Strategy for Cyberspace' an Invitation for Cooperation or a Declaration for Confrontation?" *Zhongguo Qingnian Bao* Online, 23 June 2011.

needed in search of a core value, he noted. The issue of how to respond was also the focus at a Young Computer Scientists and Engineers Forum of the China Computer Federation.[259]

After the release of William Lynn's *Strategy for Operating in Cyberspace* in July 2011, other articles ensued. Li Minghai wrote that the US desired to be the big man on the cyber campus, where it can monitor and control cyberspace at all times. The cyberspace blueprint has now become a roadmap, in Li's opinion, to boost US cyber deterrence capabilities.[260] The US possesses a cyber resource advantage in root servers that will enable it to achieve domination over other nations:

> The Internet's ability to interconnect and intercommunicate could not be accomplished without the Domain Name Server (DNS). Currently, of the 13 root DNS in the world, 10 are set up in the United States and the other three are set up in the United Kingdom, Sweden, and Japan. Through its own 'authority to regulate' and 'authority to speak' advantages, the United States anxiously desires to achieve 'network supremacy,' thereby bossing other nations around through this strategic weapon of cyberspace and consolidating its political and military positions.[261]

Other Chinese analysts also critiqued the *Strategy for Operating in Cyberspace*. One columnist stated that this policy was a major strategic step for the US, since it turned the review and discussion of cyberspace into a deployment and action activity. The strategy will organize and train the US, imbue national security with cyber deterrence capabilities, and prepare the US to fight back against any hostile cyber behavior. With regard to cyber deterrence, the strategy will develop a cyber army capable of defense and offense, will develop digital bombs, and will use real military force to attack an enemy's network when necessary. It is hard to imagine that the strategy will not lead to a cyber arms race, the columnist added, stating that "the production of cyber technological products as well as the independence and security of their application will become a prominent question."[262]

Conclusions

The rapid development of China's cyber capabilities clearly has some US analysts concerned. Bruce Goodwin, chief of Livermore Lab's weapons program, stated that "if we don't win this race [supercomputing] we're screwed. We're in a world of hurt." The US risks falling behind in the computing race at the end of this decade if serious changes and cash flows do not materialize to support an all-out effort to stay in the lead.

Several of the new organizations the PLA has developed as part of its reform

259 Ibid.

260 Li Minghai, "Ruling the Roost in Networks, the US Military Accelerates the Pace—A Cursory Discussion of the US 'Strategy for Operating in Cyberspace' Report," *Jiefangjun Bao* Online, 18 August 2011, p. 10.

261 Ibid.

262 Yu Xiaoqiu, "Cyber Deterrence is a Dangerous Game," *Renmin Ribao* Online, 25 July 2011, p. 3.

effort focus on cyber issues. These efforts represent the continuous development of a strategic, integrated, and comprehensive cyber capability. The rapid growth of these elements could imply an overall effort to impose an "information deterrence" stranglehold on the US. These new developments are buttressed by updated versions of several older concepts. For example, stratagems such as "win victory before the first battle" are mentioned as an implied cyber goal of the Strategic Planning Department. There are also cyber mobilization exercises intended to increase the capabilities of the information industry and experts; and the continuing effort to cast People's War as a viable concept under conditions of informatization.

In conjunction with China's efforts at improving its supercomputers in the future, the present battle seems to center around improving quantum computing. As a result, new and improved cyber warfare models are continuously being generated.

Overall, US analysts should be concerned about the speed and direction of China's cyber effort. They are studying US efforts in this area and are attempting to find ways to exploit US policies. They can do so without the legal limitations that are imposed on our cyber strategists. In short, in spite of our advantages we have several disadvantages that others are working to manipulate. They are attempting to establish the groundwork that will allow them to "win victory before the first battle."

PART TWO
CYBER
INTELLIGENCE ACTIVIST

CHAPTER FOUR
WESTERN REPORTS OF CHINESE CYBER ACTIVITIES: ORGANIZATIONAL ASPECTS AND CASE STUDIES

Introduction

US and other Western analysts have written on a wide range of Chinese cyber activities. US Chinese cyber experts Mark Stokes and James Mulvenon and Canadian Chinese cyber experts Rafael Rohozhinski and Ron Deibert are among the best known for their wide-ranging expertise and analysis. Other analysts have focused more specifically on the organizational structure of the Chinese General Staff or on case studies of suspected Chinese cyber intrusions. Such Western reports and case studies will be the basis of the discussion here. The overall picture is that China's massive cyber team has been extremely active and is growing at an enormous rate.

One primary activity of this growing organization has been cyber espionage. Chinese cyber reconnaissance forces, both military and civilian, have targeted numerous nations across the globe. In addition to the US, targets have included South Africa, Taiwan, South Korea, Japan, Germany, Australia, and England. China's incursions into each nation's cyber networks reflect a serious problem when viewed as part of a short-term goal of conducting "preemptive reconnaissance." This short-term goal can accommodate a longer-term goal of affecting military planning or economic development, and there are many factors indicating that this may be China's goal. A recent *Wall Street Journal* article, written by three highly influential US policy makers, indicated just how disconcerting these activities have become. The authors stressed that cyber thievery has become China's national policy, one that the US and others must challenge.[263]

China's cyber reconnaissance activities have not ceased, despite repeated warnings, further incensing nations and infusing them with scorn against the Middle Kingdom. These data-mining efforts most likely have produced some astounding results for Chinese hackers, who have moved about various sites with relative ease. Many of these activities were eventually revealed, but not until the damage was done.

What follows are some examples of Chinese activities as reported by US and other Western experts that enable the labeling of China as an intelligence or espionage activist. These experts have done an outstanding job of chronicling a massive effort aimed at sucking terabytes of information out of Western systems. The severity of the threat enhances the requirement to thwart Chinese hacker activities as soon as possible. Left untouched, the Chinese have no reason to halt their efforts to obtain crucial data on Western economic issues or to halt the theft of blueprints or technical parameters from military equipment.

263 Mike McConnell, Michael Chertoff, and William Lynn, "China's Cyber Thievery is National Policy—And Must be Challenged," *The Wall Street Journal*, 27 January 2012, p. A15.

2007: General James Cartwright

Prominent US officials have taken note of China's offensive behavior and pointed their cyber-espionage finger directly at the country. In November 2007 testimony before the US-China Economic and Security Review Commission, General James Cartwright, at the time the Vice Chairman of the Joint Chiefs of Staff, directly blamed China for cases of cyber espionage. He stated that he was particularly concerned about Chinese use of denial-of-service attacks.[264] During Cartwright's testimony, he stated:

> The data collected from these computer reconnaissance campaigns can be used for myriad purposes, including identifying weak points in the networks, understanding how leaders in the United States think, discovering the communication patterns of American government agencies and private companies, and attaining valuable information stored throughout the networks.[265]

2009: Northrop Grumman Corporation Report

In 2009 Northrop Grumman published a report that outlined several types of Chinese computer exploitation activities. The report was written at the behest of the US-China Economic and Security Review Commission and stressed the long-term nature of Chinese reconnaissance and theft activities against commercial firms.

The initial part of the report was a review of Chinese cyber policy over the past several years. This part of the report was deemed the operational strategy. It was followed by a review of Chinese computer network operations. Next the report included a review of Chinese hacker activities, which seemed to rely heavily on the research of US analyst Scott Henderson of the Foreign Military Studies Office (FMSO), as well as several Chinese reports.

The most interesting aspect of the report was its detailed account of an extensive Chinese-based cyber mission conducted against an unnamed US commercial firm a few years back. During this espionage case the Chinese utilized an extensive reconnaissance plan that must have been implemented over several months. Evidence suggesting a thorough reconnaissance effort is implied from the attackers' actions once the actual intrusion plan unfolded. They did not open and review files but, due to their successful reconnaissance effort, simply began to copy and remove the files or folders they wanted. Their reconnaissance activities were so precise that they escaped with the exact information they sought. A break-in of this nature could only have occurred after

---

264 "Report: Foreign Attacks on US Grid Increasing," 2009, *On DEADLINE*, retrieved May 5, 2009 from http://blogs.usatoday.com/ondealine/2009/04/report-foreign-attacks-on-us-grid-increasing, *Report to Congress of the US-China Economic and Security Review Commission,* June 2007.

265 Ibid., p. 12.

an accurate map was made of the network and the files.[266]

When the time came to break into the company's computer network, the cyber thieves utilized breach teams, collection teams, exfiltration teams, and intermediate "staging servers," among other issues. The Northrop Grumman report notes that "the exfiltration operation indicates that their command and control architecture relied upon previously stolen valid user accounts to authenticate to the company's internal servers."[267] This was a sophisticated effort that required the acquisition of specific user IDs and protocol information. It resulted in a spectacular theft of intellectual property.

2009: Tracking Ghostnet: Canadian Report on Cyber Espionage

The Canadian-based *Information Warfare Monitor* produced a detailed report on Chinese cyber spying around the Middle Kingdom's periphery. A collective of analysts published the results of a ten-month-long investigation that centered on accusations of Chinese cyber espionage against Tibetan institutions and others. As the study's foreword notes, "attributing all Chinese malware to deliberate or targeted intelligence gathering operations by the Chinese state is wrong and misleading."[268] However, when digital natives within China are included in the assessment, strong circumstantial evidence points to the People's Republic of China as the main culprit.

The study's findings state that a significant attacker IP address traces back to Hainan Island in China. The island is the reputed home of the Lingshui signals intelligence facility of the People's Liberation Army (PLA). The authors note the following:

> The most obvious explanation, and certainly the one in which the circumstantial evidence tilts the strongest, would be that this set of high profile targets has been exploited by the Chinese state for military and strategic-intelligence purposes. Indeed, as described above, many of the high confidence, high-value targets that we identified are clearly linked to Chinese foreign and defense policy, particularly in South and South East Asia.[269]

The espionage network includes 103 countries and over one thousand infected computers, nearly a third of which were high-value targets (embassies, consulates, etc.). The authors add that while China appears to be the main culprit, it is not inconceivable that the network was established by another state and operated within China. However the chances are greater that Chinese citizens were involved in the affair.

---

266 Bryan Krekel (Principal Author), *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*, a report prepared for the US-China Economic and Security Review Commission, October 9, 2009, pp. 59-63.

267 Ibid.

268 Ron Deibert and Rafal Rohozhinski, *Tracking GhostNet: Investigating a Cyber Espionage Network*, Information Warfare Monitor, 29 March 2009, Foreword.

269 Ibid., p. 48.

2011: The PLA's Signals Intelligence and Cyber Reconnaissance Infrastructure

The extent of China's organizational development of cyber reconnaissance assets was highlighted in the report *The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure*.[270] Authors Mark Stokes, Jenny Lin, and L. C. Russell Hsiao, writing for the Project 2049 Institute, explain in depth the wide-spread capability of the PLA to collect information on other countries. The report discusses both the Third Department (signals intelligence collection, cryptology, computer security, and analysis agency) and the Fourth Department (radar, electronic support measures, electronic warfare, electronic intelligence, and electronic countermeasures). Only the Third Department is discussed here. The person believed to be serving as the director of the Third Department is Major General Meng Xuezheng.

Stokes, Lin, and Hsiao note that the Third Department discussion is tentative and theoretical. They divided their study into two parts: command structure and subordinate research institutes; and the department's twelve operational bureaus. The command has a headquarters, political department, logistics department, science and technology intelligence bureau, and science and technology equipment bureau. Key subordinates to the Department include the 56th Research Institute (supercomputing), the 57th Research Institute (communications intercepts, signal processing, and satellite communications), and the 58th Research Institute (cryptology, information security technology).[271]

The operational bureaus of the Third Department are organized as follows:

- 1st Bureau (61786 Unit)—decryption, encryption, information security
- 2nd Bureau (61398 Unit)—US and Canada focus
- 3rd Bureau (61785 Unit)—line of sight radio communications, direction finding, emission control
- 4th Bureau (61419 Unit)—Japan and Korea focus
- 5th Bureau (61565 Unit)—Russia focus
- 6th Bureau (61726 Unit)—no mission given; Wuhan U. network attack and defense center is located in this area of operation
- 7th Bureau (61580 Unit)—some computer network attack and computer network defense, some work on the US network-centric concept, psychological and technical aspects of reading and interpreting foreign languages
- 8th Bureau (61046 Unit)—Western and Eastern Europe, Middle East, Africa, Latin America
- 9th Bureau (unknown Unit)—strategic intelligence analysis/data base management, the most opaque bureau
- 10th Bureau (61886 or 7911 Unit)—Central Asia or Russia, telemetry missile tracking, nuclear testing

270 Mark A. Stokes, Jenny Lin, and L.C. Russell Hsiao, *The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure*, Project 2049 Institute, November 2011.

271 Ibid., pp. 4-5.

- 11th Bureau (61672 or 2020 Unit)—Russia
- 12th Bureau (61486 Unit)—satellites, space-based signals intelligence (SIGINT) collection.[272]

These operational bureaus, according to the report, are separate from the technical reconnaissance bureaus (TRB) under the seven military region headquarters. The TRBs of the military regions (MRs) include the following responsibilities:

- Beijing MR (66407 Unit)—Russia, along the Inner Mongolian border
- Chengdu MR (78006 and 78020 Unit)—2 TRBs; English, computer network exploitation operations
- Guangzhou MR (75770 Unit)—Internet viruses, voice over Internet protocol
- Jinan MR (72959 Unit)—oversees 670 technical specialists, microwave relay intercepts, Korean, Japanese, English, and other language specialists
- Lanzhou MR (68002 and 69010 Units)—monitor border military activities
- Nanjing MR (73610 and 76630 Units)—Western Pacific, Taiwan
- Shenyang MR (65016 Unit)—Russia, Korea, Japan targets.[273]

Finally, the report listed several organizations associated with the Third Department. The PLA's Information Engineering University is the Third Department's training vehicle. According to the report, other organizations associated with computer network defense are:

- PLA Communications Security Bureau
- China North Computation Center
- Third Department Computing Center
- National Research Center for Information Security Technology (Network Risk Assessment)
- PLA Information Security Evaluation and Certification Center
- Information Security Research Institute
- National Information Center (affiliated with science and technology equipment)
- National Information Security Engineering Technology Center.[274]

This is an outstanding report that should be bookmarked.

2011: Night Dragon, Shady Rat

US civilian analysts in particular highlighted two Chinese reconnaissance activities during the past four years. These espionage efforts were dubbed Night Dragon and

272 Ibid., pp. 7-11.
273 Ibid., pp. 12-13.
274 Ibid., pp. 5-6.

Shady Rat. The US security vendor McAfee helped uncover these intrusions.

The "Night Dragon" operation took place over a period of "at least two years and likely as many as four,"[275] and targeted the oil, gas, and petrochemical companies. There apparently were three major steps in the operation. First, public websites were defaced using Structured Query Language (SQL) injections (hackers attempt to acquire databases in response to commands that usually are blocked). Second, once compromised, programs such as remote administration tools (RAT) were uploaded. These tools allow access to machines. Third, hackers then browse directories and use password-cracking tools to get access to services containing sensitive information.[276]

Dmitri Alperovitch, then vice president of threat research at McAfee, stated that the infiltrators were extremely sloppy in their efforts, leaving much evidence behind as to the origin of the attack. To Alperovitch this was an attempt at energy espionage that was not nearly as sophisticated as the Aurora infiltration of Google or the Stuxnet operation aimed at Siemens equipment running Iran's nuclear facility.[277]

A *McAfee White Paper* later identified one individual who appeared to have extensive knowledge of the infiltration. That person is based in Heze City, Shandong Province, China. This individual runs a company that provides "hosted servers in the US with no records kept" for $10 a year for 100MB of space.[278]

The Symantec Corporation's analysts also weighed in on this individual, to whom they gave the pseudonym of Cover Grove, the literal transliteration of his name. They noted that the infiltration was traced to a virtual private server (VPS) located in the US but owned by a 20-something male located in the Hebei region of China. The individual specialized in network security. Allegedly the US-based VPS was for logging into the QQ instant messaging system of China. When asked about hacking skills, the individual provided a contact who performed "hacking for hire." Symantec ended its analysis noting that "nor are we able to definitively determine if he is hacking these targets on behalf of another party or multiple parties" and "we are unable to determine if Cover Grove is the sole attacker or if he has a direct or only indirect role."[279]

The Chinese, of course, denied any involvement in the espionage effort. Li Wei, a security expert at China's Institute of Contemporary International Relations, was representative of the Chinese response. He stated that the accusations were "unprofessional" and "irresponsible."[280]

Operation Shady RAT (remote access tool) was another purported example of Chinese espionage. McAfee again produced the initial report, one which did not accuse

275 Jeremy Kirk, "'Night Dragon' Attacks from China Strike Energy Companies," *IDG News Service*, 10 February 2011.

276 Ibid.

277 Gregg Keizer, "'Sloppy' Chinese Hackers Scored Data-Theft Coup with 'Night Dragon'," *Computerworld* Online, 11 February 2011.

278 William Pentland, "Night Dragon Attacks Target Technology in Energy Industry," *Forbes*, 19 February 2011.

279 Eric Chien and Gavin O'Gorman, "The Nitro Attacks: Stealing Secrets from the Chemical Industry," *Symantec Security Response*, 2011.

280 Wang Zhaokun, "Chinese Hackers 'Hit Western Oil Firms,'" *Global Times* Online (in English), 11 February 2011.

China directly. Rather, the report's author noted that "what I have described here has been one specific operation conducted by a single actor/group."[281] Other analysts, such as cyber security expert James Lewis of the US Center for Strategic and International Studies, weighed in on the report. Most analysts pointed their espionage fingers directly at China. Bruce Sterling, writing at *Wired.com* about the McAfee report, stated the following:

> Cyber espionage is an aspect of Chinese soft power. It is part of an advantage their covert, disciplined, and centralized system possesses, which the globalized, flat-world system of the Washington Consensus simply lacks. It is just a unique Chinese strategic advantage. The rest of us are no more likely to combat this situation than we can combat global warming.[282]

The operation discussed advanced persistent threats that generally occur without public disclosures. Over the past five to six years, the report notes, nothing short of a historical transfer of wealth has occurred. Items stolen include national secrets, source codes, databases, e-mail archives, negotiation plans, exploration details for energy activities, document stores, legal contracts, supervisory control and data acquisition configurations, design schematics, and more. The adversary is interested in secrets and intellectual property and not the financial gratification driving cybercrime.[283] In all, the report dissected intrusions at more than 70 global companies, governments, and nonprofit organizations during the last five years.

2011: An Australian's Perspective

Australian electronic warfare expert Desmond Ball has written an exhaustive article outlining China's cyber warfare activities. He highlights the numerous cyber activities that have taken place over the past several years and lists the names of selected Chinese computer viruses and worms at the end of the article.[284]

Using a host of Western and Asian sources, Ball highlights the many attempts the Chinese have made to infiltrate other nations' cyber systems. Some of these activities are intelligence operations that were uncovered by numerous other nations, such as England. Further, he discusses the many attempts that China's netizens have made on behalf of nationalist causes, to include attacks on Japan, NATO, Taiwan, and other countries. Finally, Ball cites reports indicating that China has its own cyber vulnerabilities with which to contend. A report from PC1News.com noted that China was the country most affected by the top 100 viruses infecting computers world-wide.[285]

281 Dmitri Alperovitch, "Revealed: Operation Shady RAT," *McAfee White Paper*, 2011, p. 14.

282 Bruce Sterling, "Operation Shady RAT," *Wired.com*, 3 August 2011, at http://www.wired.com/beyond_the_behond/2011/08/operation-shady-rat/

283 Alperovitch, "Revealed…," p. 2.

284 Desmond Ball, "China's Cyber Warfare Capabilities," *Security Challenges*, Volume 7 No. 2 (Winger 2011), pp. 81-103.

285 Ibid., especially p. 98 for the virus information.

If there was a question mark for analysts regarding Ball's article, it would be his finding that "There is no evidence that China's cyber-warriors can penetrate highly secure networks or covertly steal or falsify critical data."[286] Further, to state that China is "condemned to inferiority in IW capabilities for probably several decades"[287] leaves the reader wondering about the data located in the rest of his article, which appeared to state just the opposite. In fact, Ball generously quotes from the Northrop Grumman report that offers a case study regarding how Chinese hackers made off with precision-targeted files using various escape mechanisms. He also notes that China was able to penetrate the computers of Google, Lockheed Martin, and several energy companies. Such work is not a product of the uninformed. China has clearly penetrated numerous computer systems around the world.

A recent report from the Office of the National Counterintelligence Executive also contradicts Ball's conclusions. The report judges that China will remain an aggressive and capable collector of sensitive US economic information and technologies, especially in cyberspace.[288]

2012: A Second Northrop Grumman Corporation Report

Northrop Grumman Corporation prepared its second report for the US-China Economic and Security Review Commission in March 2012. Titled "Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage," the work by Bryan Krekel, Patton Adams, and George Bakos is an excellent summary of information warfare doctrine, China's projected wartime use of computer network operations, and the key entities (universities, institutes) that conduct such research in China.

The report states that China is attempting to unify its information warfare strategy within a concept known as "information confrontation" where electronic and non-electronic capabilities are merged. This is a departure, the report adds, from the earlier concept known as integrated network-electronic warfare or INEW. Centers of gravity appear to remain adversary command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) systems and logistics. The report also identifies some 50 civilian universities that are conducting information security research programs for the PLA. A warning is issued about the close connection between China's telecommunications hardware manufacturers and US supply chains that could create a penetration vector for Chinese espionage. The report notes, however, that "no evidence for such a connection is publicly available."[289] The report, like its predecessor, should be mandatory reading for anyone interested in the intricacies of Chinese cyber

286 Ibid., p. 101.

287 Ibid.

288 "Foreign Spies Stealing US Economic Secrets in Cyberspace*," Security Counterintelligence*, Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011, from the Office of the National Counterintelligence Executive, October 2011, p. ii.

289 Bryan Krekel, Patton Adams, and George Bakos, "Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage," Northrop Grumman, 7 March 2012, pp. 8-10.

operations.

2012: A PLA Cyber Militia Case Study

Policy analysts Robert Sheldon and Steven Glinert wrote a detailed study examining Chinese cyber groups that have been understudied or even overlooked by analysts. These groups are known as cyber militias and are part of a civil-military integration process in China that leverages procurement relationships and outsourcing arrangements. The responsibilities of cyber militias appear directed more toward defensive activities than any other type of operation.[290] The 2009 Northrop Grumman report was the only other recent source to mention these groups in some detail.

The authors write that the eight-million strong militia system (defined as an armed organization composed of the masses not released from their regular work) in China is where the cyber militia component can be found. Sheldon and Glinert have with great care painstakingly uncovered sixty-four groups designated in the Chinese language as either information militias or network militias. The relationship of the groups to Chinese developmental programs and High Tech Development Zones along with their mobilization potential, possible wartime roles, geographic dispersion, and functions, roles, and missions are discussed.

The authors conclude that cyber militias are not serving at the core of China's operational cyber forces but are instead performing several related missions such as training PLA operators. Cyber militias also have the potential to perform defensive operations in wartime and peacetime. Further, the presence of cyber militias in universities and businesses in China should serve as a "buyers beware" sign for US companies. Sheldon and Glinert's article is well-worth the time to find and read. It is a one of a kind item.

Conclusions

The studies cited above indicate not only the widespread nature of the Chinese cyber intrusion pattern in countries around the world, but also offer insights to the vast nature of this cyber machine. Departments within the Chinese General Staff, surrogate hackers or those directed by the communist party, cyber militias, and other elements (Telecom supply chains, etc.) indicate the complexity of the beast.

The ability of Chinese hackers to gain administrative control over certain systems and prepare them for focused stealth activities has enabled the targeted penetration of specific systems. The hackers, in turn, walk away with terabytes of information. Several of the most important US systems have been penetrated in such a manner. Further, the Chinese continue to expand their cyber activities and ignore the warnings of other countries at great risk. It was perhaps for this reason that the US published its cyber security strategy and warned that certain attacks against its infrastructure would elicit

290 Robert Sheldon and Steven Glinert, "Civil-Military Integration and China's Cyberspace Operations: A Case Study on PLA Cyber Militias," working paper for the "Conference on China and Cybersecurity," 11-12 April 2012. Used with the author's permission.

US attacks of both a cyber and noncyber nature in retaliation.

CHAPTER FIVE
GOOGLE CONFRONTS CHINA: A CYBER CASE STUDY

Introduction [291]

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

> A person with direct knowledge of the investigation now says that the losses included one of Google's crown jewels, a password system that controls access by millions of users worldwide to almost all of the company's Web services, including e-mail and business applications. The program, code named Gaia for the Greek goddess of the earth, was attacked in a lightning raid taking less than two days last December, the person said.[292]

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

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

Why America Has Had Enough

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

---

291 This article originally appeared in the Summer 2010 issue of *Parameters*, pp. 101-113. It is slightly edited in this version.

292 John Markoff, "Cyberattack on Google Said to Hit Password System," *The New York Times*, 19 April 2010, http://topics.nytimes.com/2010/04/20/technology/20google.html?_r=1ref=john_markoff,A1.

- 2004: Titan Rain, FBI name for a group of hackers from Guangdong Province who stole information from US military labs, NASA, the World Bank, and others.
- 2006: A US State Department official in East Asia opens an e-mail that allows hackers to break into computers at US embassies all over the region.
- 2006: Representative Frank Wolf's office is attacked. He is an outspoken lawmaker on Chinese human rights issues and suspects the Chinese in the attack.
- 2006: the US Commerce Department had to throw away all of its computers due to targeted attacks originating from China.
- 2006: the Naval War College took all of its computers offline after a major cyber attack in which China emerged as the main culprit.
- 2007: Commerce Secretary Carlos Gutierrez finds spy software on his computer following a trade mission trip to China.
- 2008: The presidential campaigns of both President-elect Barack Obama and Senator John McCain are attacked by Chinese cyber spies.
- 2009: Senator Bill Nelson revealed attacks against his computer had been traced to China.
- 2009: Toronto researchers find a massive cyber espionage ring using Chinese malware they call Ghostnet. The attacks penetrated 103 countries and their origin was China.
- 2009: Lockheed Martin's F-35 program is hacked and China emerges as the main suspect.[293]

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

How Serious was the Google Attack?

The attack on Google occurred in December 2009. Some sources state that as many as 33 companies were victims of the hack attack. Alan Paller, the director of the well-known information security training firm known as the SANS Institute in Bethesda, Maryland, indicated just how invasive the attacks were, noting "the odds of the 25 biggest companies in California not being fully compromised by the Chinese is near zero."[294] His analysis indicates the probes were serious and highly effective. Fully compromised? One hopes that Paller was exaggerating the threat, but there are many reasons to believe he was not.

The attack itself on Google was so out of context, so odd, that US Chinese cyber

293 Josh Rogin, "The Top Ten Chinese Cyber Attacks (that we know of)," Foreign Policy (Cable), 22 January 2010, http://thecable.foreignpolicy.com/posts/2010/01/22/the_top_10_chinese_cyber_attacks_that_we_know_of, accessed 21 February 2010.

294 Jessica Guynn, "Chinese Hackers Pose a Growing Threat to US Firms," T*he Los Angeles Times*, 15 January 2010, at http://articles.latimes.com/2010/jan/15/business/la-fi-google-china15-2010jan15.

expert James Mulvenon called the event a "watershed moment in the cyber war."[295] Perhaps this was because the attack focused on commercial firms, which had appeared to be a secondary option of the Chinese in past attacks. Or perhaps it was because this was the first time a commercial firm, Google, had actually come forward and admitted they were under attack. Past practices had witnessed commercial companies and banks remaining quiet when experiencing cyber attacks in an attempt to retain consumer confidence. The Pentagon, on the other hand, has been quicker to move and announce probes against their systems.

Acts of commercial espionage indicate that the Chinese are looking as closely at economic secrets as they are at military or diplomatic secrets. Perhaps, after the thousands of attacks already attributed to China, Chinese hackers have accomplished everything they wanted in government spheres and have moved on to bigger prizes. Or perhaps they simply have decided to alter their target methodology. In addition to Google, Adobe Systems, Rackspace Hosting, and the Santa Barbara, California, software maker CyberSitter all reported attacks.[296] Sometime later the law firm Gipson Hoffman & Pancione (representing CyberSitter and Symantec), Juniper Networks, Northrop Grumman, Yahoo, and Dow Chemical also reported hits by the attackers.[297]

A few months earlier, Northrop Grumman had published a report, written at the behest of the US-China Economic and Security Review Commission, which outlined various Chinese computer exploitation activities. It indicated that Chinese activities against commercial firms have been ongoing for quite some time. In particular, the report detailed an extensive Chinese-based cyber mission conducted against an unnamed US commercial firm a few years earlier. During this espionage case the Chinese utilized an extensive reconnaissance plan against the company that continued over a number of months. Evidence suggesting a thorough reconnaissance effort can be implied from the attackers' actions once the actual intrusion plan unfolded. The perpetrators did not open and review files but, due to their successful reconnaissance effort, simply began to copy and remove the files or folders they wanted. Their reconnaissance activities were so precise they were successful in stealing the information they sought. A break-in of this nature could only have occurred after an accurate map was made of the targeted network and files.[298]

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

295 Ibid.

296 Ibid.

297 Kelly Jackson Higgins, "More Victims of Chinese Hacking Attacks Come Forward," *DarkReading*, 14 January 2010, part of a compilation of reports published as "Google's China Affair," *InformationWeek Analytics*, 29 January 2010.

298 Bryan Krekel, *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation* (Washington: US-China Economic and Security Review Commission, 9 October 2009), pp. 59-63.

servers."[299] This was a sophisticated effort that acquired specific intellectual property.

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

Who Attacked Google?

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

Initially, the journalists noted the US National Security Agency and other computer-security firms traced the attacks to servers in Taiwan. Then, citing "people involved in the investigation," they reported that the attacks were traced to two educational institutions in China. The journalists reported that a US defense contractor that had been subject to attacks similar to those that Google experienced had identified an unusual suspect, a Ukrainian professor teaching at a Chinese vocational school, as the source behind the attacks.[300]

The Chinese institutions involved were identified as the Shanghai Jiaotong University and the Lanxiang Vocational School. The journalists noted that these institutions may have been used as fronts for government agencies.[301] Markoff and Barboza also conferred with Mulvenon and discovered that the Chinese have a different model for computer network exploitation operations. These operations incorporate volunteer "patriotic hackers" in support. Other Chinese experts told the journalists that China has a highly distributed approach to online espionage that makes it impossible to prove where attacks originate.[302]

An interesting part of the article was the journalists' ability to conduct interviews with two Chinese professors at Jiaotong University. One professor said that an internal investigation at the university had already started. The other said it was possible someone from the university was involved, since an individual could commit an act of wrongdoing, or possibly the university Internet Protocol address was hijacked. Jiaotong is no ordinary university. It has ties with several US universities, to include Duke and the University of Michigan, and to various US commercial entities such as Microsoft and Cisco Systems. Jiaotong received funding from Chinese Project 863 (China's Information Technology Security Plan), has a School of Information Security Engineering, and has People's Liberation Army ties, according to the university's Web site. It has also hosted prominent Chinese hackers for lectures.[303] At least one of these

299 Ibid.

300 John Markoff and David Barboza, "Two Chinese Schools Said to Be Tied to Online Attacks," *The New York Times* Online, 18 February 2010, located at http://www.nytimes.com/2010/02/19/technology/19china.html?emc=eta1nyt.com.

301 Ibid.

302 Ibid.

303 David Barboza, "Hacking Inquiry Puts China's Elite in New Light," *The New York*

hackers is anti-Western and believed to have previously worked for Google.

A representative from the other school, the Lanxiang Vocational School, said he doubted whether any of the high school graduates at his school had the ability to hack Google or any other company. This may be a bit of an understatement, since the school's computer laboratory is so enormous that it was listed in the *Guinness Book of World Records*. The school's Web site states that it sends a number of graduates to the armed forces. The school's dean, Mr. Shao, said graduates of the school's computer science department are recruited by the local military on an annual basis.[304]

Barboza and Markoff added that other computer industry executives (and former government officials) said it "was possible that the schools were cover for a 'false flag' intelligence operation being run by a third country."[305] Or, perhaps, the attacks were the responsibility of criminal elements dealing in industrial espionage.[306] Thus, at the end of their article, the reader is wiser but still not certain as to who committed the attacks. The majority of the evidence, however, indicts China.

Chinese Responses to Google's Accusations

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

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

An analysis of the aftermath of the Google probes provides an example of this process. The initial Chinese responses to Google's accusations were offered by many of the same agencies that the Chinese have used in the past. Initially, a Foreign Ministry spokesman (Ma Zhaoxu) said, "foreign enterprises in China need to adhere to China's laws and regulations, respect the interests of the general public and cultural traditions,

---

Times, 22 February 2010, located at http://www.nytimes.com/2010/02/22/technology/22cyber.html?ref=technology

304 Ibid.

305 Markoff and Barboza.

306 Ibid.

and shoulder corresponding responsibilities. Google is no exception."[307] Ma did not indicate that China would investigate Google's accusations nor did he mention the grounds for Google's decision to remove censorship, namely that someone in China had attacked its infrastructure. Chinese authorities dismissed the accusations as groundless. Psychologically, Ma used the stratagem of diverting attention away from the real issue under consideration, the probes, and redirected the focus to various legal issues.

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

And what was the Chinese response to Secretary Clinton's statement? The *Zhaoxu News Agency* said Clinton's singling out China was inappropriate and misguided and constituted an inappropriate meddling in Chinese affairs.[308] Again, who was meddling in whose affairs? Another Foreign Ministry spokesman, Jiang Yu, said, "China's Internet is open" and China "welcomes international Internet corporations to do business in China in line with the law."[309] Such subjective responses are specifically designed to undermine the accuser's line of reasoning.

Next, in typical Marxist-Leninist fashion, the Chinese relied on the old "counterpoint" tactic from the Communist playbook. Google accused the Chinese of collecting data on human-rights advocates, so China accused the United States of human-rights violations in one of its responses. Then, since Google and other US journalists implied Chinese government collusion in the espionage activities, the Chinese next implied White House collusion in using commercial markets (such as Google) for political purposes, yet another counterpoint tactic. A *China Daily* Internet commentary noted that four of Google's former executives hold positions in the US government, to include Sumit Agarwal, now a Deputy Assistant Secretary of Defense for Public Affairs Outreach and Social Issues.[310] The commentary went on to note that Google was the fourth-largest contributor to President Barack Obama's presidential campaign. Counterpropaganda today is perhaps an element of what might be termed

307 John Swartz, "Google Delays Launch of Two Phones in China," *USA Today.com,* 20 January 2010, p. B3.

308 Paul McDougall, "China Defends Great Firewall," *Information Week.com*, 22 January 2010, http://www.informationweek.com/news/government/policy/showArticle.jhtml?articleID=222400246.

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

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

soft psychological power.

Foreign Ministry spokesmen were not the only ones to address Google's accusations against the Chinese. Several military officials also joined in the renunciation and diversion. Huang Xueping, a Defense Ministry spokesman, stated that Google's claims were baseless, irresponsible, and hyped with ulterior motives.[311] Li Daguang of National Defense University stated that some Western powers had adopted a strategy to sabotage China's information technology development and that their high-profile criticism is a preemptive strike on China.[312] Li Yizhong, Minister of Information and Technology, stated that Google must obey China's laws and that China opposes hacking.[313] While many more defensive accusations were levied at Google, the three mentioned here represent the categories of media, psychology, and law. Other sources used to put out the official propaganda ranged from representatives of the Academy of Military Science to publications such as the *Central Party School*.

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

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

Monitoring and control groups were told to immediately conduct follow-up and control actions; not to participate in Google's information releases; not to report that Google is exerting pressure on China; and not to provide materials for Google to attack relevant policies.[314] Such instructions are representative of standard Chinese propaganda practices.

David Berlind, writing for *Information Week*, felt the US response (excluding Secretary Clinton's) to Chinese actions was "wimpy." He wrote that the response indicated that the United States fears China, since the latter now holds a winning hand for four reasons: the United States needs China to support our growing national debt; we need China to manufacture much of what we consume; we depend on the growth of China's economy for our growth, since we have little domestic production; and we need

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

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

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

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

China to keep North Korea in line.[315] The longer Western nations take to send a strong message to the Chinese, the more credible Berlind's accusation appears. Secretary Clinton's initial response was the quickest and most pointed to date.

Chinese Thinking Adapts to the Digital Age

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

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

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

Prominent US officials have taken note of this offensive behavior and pointed their cyber-espionage finger directly at China. In November 2007 testimony before the US-China Economic and Security Review Commission, General James Cartwright, then Vice Chairman of the Joint Chiefs of Staff, blamed China for cases of cyber-espionage. He was particularly concerned about China's use of denial-of-service attacks.[316] During Cartwright's testimony, he stated:

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

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

> The data collected from these computer reconnaissance campaigns can be used for myriad purposes, including identifying weak points in the networks, understanding how leaders in the United States think, discovering the communication patterns of American government agencies and private companies, and attaining valuable information stored throughout the networks.[317]

Both civilian and military Chinese sources have written about this growing cyber offensive, particularly regarding its economic nature. The journal *China Military Science* has devoted a number of articles to topics associated with Internet warfare and China's interest in developing offensive cyber options. In 2009 Senior Colonel Wang Wei, a professor at the Nanjing Military Academy's Information Warfare and Command Department's Military Theory Teaching and Research Office, and Major Yang Zhen, a lecturer at the same office, noted that a sovereign state's political system, economic potential, and strategic objectives will be the primary targets attacked in any war against an informatized society. The authors advocated that it is necessary to "defeat the superior with the inferior" and "fight in a way different from how the adversary acts," once again referencing stratagems to buttress their arguments and activities.[318] They espoused that in peacetime the organized integration of military and economic effects must be achieved; and that in People's War under informatized conditions, both financial and trade warfare must be carried out.[319] Such writings can be interpreted to mean that at least some military officers consider that China is currently at war on the Internet.

In another 2009 *China Military Science* article, Colonel Long Fangcheng and Senior Colonel Li Decai analyzed the role of soft power and its impact on what the Chinese term "comprehensive national power." Regarding the use of soft power as an economic tool, the authors suggest:

> Information and information systems are weapons…. Paralyzing the enemy country's economy, causing social turmoil to the enemy country, imposing the will of war on the opponent does not lead to large-scale engagements in a traditional sense, and can be effected in a form of soft attacks through network attacks, hacker invasions, and large-scale media warfare, psychological warfare, and legal warfare through news media. Thus the boundary between the state of peace and the state of war will become fuzzy.[320]

Fangcheng and Decai appear to be making the mistaken assumption that an attack

317 Ibid., p. 12.

318 Wang Wei and Yang Zhen, "Recent Developments in the Study of the Thought of People's War under Informatized Conditions," *China Military Science*, No. 2 2009, pp. 145-151.

319 Ibid.

320 Long Fangcheng and Li Decai, "On the Relationship of Military Soft Power to Comprehensive National Power and State Soft Power," *China Military Science*, No. 5 2009, pp. 120-129.

on another nation's economy will not lead to any large-scale response. This is dangerous thinking on the part of the Chinese. There is a threshold at which America and other nations will rapidly respond. Perhaps this conclusion is based on the current weak responses of nations.

An example of a civilian source that emphasizes economic and digital issues is the Chinese book *Internet Wars*. It also focused on the Internet confrontation in general. The book has 18 chapters. Several chapters draw the reader's attention immediately. They are: "The Inevitable Internet War," "Battles for Internet Control," "Offensive and Defensive Internet Wars," "The Internet Will Determine Victory in Future Wars," "Dangerous Virtual Reality," and "Financial Wars in the Internet World."[321] The latter should be of particular interest to US analysts.

Dr. Joel Brenner, who worked for the Director of National Intelligence from February 2007 to January 2009, has called China's economic espionage against the United States a national security risk.[322] The United States is, however, initiating actions to confront this risk. In April 2009 the Office of the Secretary of Defense hosted an information warfare simulation focusing on financial attacks on the US economy and the consequences of manipulating financial markets. China, according to one account, proved to be the "savviest economic warrior." Financial specialist Paul Bracken, one of the participants, was worried over the possibility that China might incrementally sell dollars in an attempt to increase economic uncertainty in the United States.[323]

Meanwhile, evidence continues to grow from a number of sources regarding China's economic superiority. Chinese military experts Qiao Liang and Wang Xiangsui, authors of the highly popular and controversial work *Unrestricted Warfare*, have written in another book that the control of the world economic sector has become a goal for the Chinese. They noted that "war with the objective of expanding territory has already basically withdrawn from the state of history, and even war with the objective of fighting for natural resources is now giving way to war with the objective of controlling the flow of financial capital."[324]

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

China is not overly concerned with privacy issues as we are in the United States.

---

321 Dong Niao, *Internet Wars* (Beijing: Jiuzhou Press, 2009), pp. 3-7.

322 Shane Harris, "China's Cyber-Militia," *National Journal*, 31 May 2008, http://www.nationaljournal.com/njmagazine/print_friendly.php?ID=cs_20080531_694.

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

324 Qiao Liang and Wang Xiangsui, "Fully Calculating the Costs and profits of War," in *On the Chinese Revolution in Military Affairs*, editor Shen Weiguang (Beijing: New China Press, 2004), pp. 105-112.

In fact, the state has the preponderance of control over individual cyber rights. This permits the Chinese government to act freely regarding the management of information or its monitoring. The Chinese can establish their own rules for anything they claim to own. This translates into myriad trade restrictions and tariffs, not to mention the undervaluing of the Yuan. Outside agencies and customers complain that doing business with China means putting up with their insistence on controlling such activities and actions as foreign encryption protocols companies use to protect sensitive data. Certifications to do business on the mainland are held up until companies comply with Chinese demands, according to Oded Shenkar, a business management professor at The Ohio State University.[325] A 2009 report from the European Union's Chamber of Commerce in China noted that China integrated requirements guaranteeing protectionism into various standardization policies required for the subjective enforcement of environmental rules favoring Chinese firms. Such policies make it much easier to commit the theft of intellectual property.[326]

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

Conclusions

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

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

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

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

326 Ibid.

CHAPTER SIX
RECONNAISSANCE ENABLES CYBER CONTROL

Information and information systems are weapons…Paralyzing the enemy country's economy, causing social turmoil to the enemy country, imposing the will of war on the opponent does not lead to large-scale engagements in a traditional sense, and can be effected in a form of soft attacks through network attacks, hacker invasions, and large-scale media warfare, psychological warfare, and legal warfare through news media. Thus the boundary between the state of peace and the state of war will become fuzzy.[327]

Introduction

Three Chinese military concepts, *shi*, war control, and, to a lesser degree, war engineering are likely conceptual resources motivating many of China's electronic reconnaissance activities against nation states. By uncovering vulnerabilities in opposing systems, reconnaissance activities allow a force to properly prepare for a wartime mission in peacetime and help them establish a strategic advantage. They allow a distant force to prepare for close virtual combat, much like a digital puppet master whose electronic strings allow him to open and close enemy vulnerabilities at will.

It is important for Western audiences to become familiar with these and several other Chinese theoretical topics if they are to comprehend what is behind the extended military and civilian reconnaissance efforts of the Chinese. Viewed separately and out of context they are less threatening than when viewed within an integrative purpose and methodology.

This chapter will summarize these Chinese concepts and the role they play in laying the groundwork for "winning victory before the first battle." Understanding these concepts should help Western analysts better comprehend indicators leading to the unveiling of China's strategic intent as it prepares its forces for twenty-first century contingencies.

The *Shi* of Virtual Reality

Shi is an important strategic Chinese concept with roots as far back as the title of Chapter Five of Sun Tzu's classic *The Art of War*. One US source defines *shi* as the strategic configuration of power or advantage.[328] Tao Hanzhang, a retired Chinese General, defines *shi* as "the strategically advantageous posture before a battle that enables it to have a flexible, mobile, and changeable position during a campaign."[329]

327 Long Fangcheng and Li Decai, "On the Relationship of Military Soft Power to Comprehensive National Power and State Soft Power," *China Military Science*, 5-2009, pp. 120-129.

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

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

Another Chinese source, the book *Campaign Stratagems*, defines *shi* as the combination of the friendly situation, enemy situation, and the environment; as the sum of all factors impacting the performance of the operational efficiency of both sides; and as the key factor determining the rise and fall of operational efficiency.[330]

The term *shi* (pronounced like the English word "sure") appears eighty or more times in Chinese dictionaries and each time it is expressed by a different Chinese character with a different meaning (but is pronounced the same except for tonal stress).[331] *Shi* can be expressed linguistically via four tones, which are: neutral, ascending, descending, or descending-ascending. For each tone there are twenty or so different Chinese characters. For example, the words ten, teacher, non-commissioned officer, time of day, to begin, to be, to test, to make, to see, to know, room, and thing are all pronounced via one of the four tones of *shi*. Each one is expressed/written with a different Chinese character. Therefore it is important to know just which Chinese character of *shi* one is speaking about and defining. In the case for this article, we are using the *shi* character for strategic advantage.

The same character for *shi* that has been translated as strategic advantage has been translated in other ways by various translators. Some of the translations of this character are energy, potential, force, disposition, and momentum.

Virtual or electronic *shi*, then, is the attainment of electronic potential expressed as strategic advantage. US Defense Officials recognize Chinese attempts to realize virtual *shi* in today's digital environment implicitly more so than explicitly. For example, Richard Lawless, US Deputy Undersecretary of Defense for Asia-Pacific affairs, told Congress in 2007 that the Chinese military's "determination to familiarize themselves and dominate to some degree Internet capabilities—not only of China and that region of the world—provides them with a growing and very impressive capability that we are very mindful of and are spending a lot of time watching."[332] The ability to dominate enables the attainment of a strategic advantage.

The apparent goal of the PLA's newly-developed digital quantum leap is to allow it to be fully prepared to achieve virtual or electronic *shi* early in the twenty-first century. A virtual advantage could be attained by uncovering vulnerabilities in a potential enemy's digital systems through reconnaissance activities or by planting computer viruses in such systems. Uncovering weaknesses in peacetime would allow the PLA to gain an initial advantage if war broke out. Only by attaining virtual *shi* can the PLA "win victory before the first battle." Achieving such advantages requires updating the PLA's thinking by adding "informatized" modes of thought.

It is the *shi* of virtual reality or informatized *shi* that should concern cyber analysts today. The Chinese have written about the disposition and potential of electrons for years. In the information age, strategic advantage can be obtained quickly from long

330 Zhang Xing Ye and Zhang Zhan Li, editors, *Campaign Stratagems*, National Defense University, 2002, pp. 8-18.

331 Discussion with Chinese language instructors Marn-Ling Wang and David Dai at the US Defense Language Institute, July 2009.

332 John Tkacik, *Trojan Dragons: China's International Cyber Warriors*, WebMemo, 2007.

distances, even from distant continents, whether it be via a computer virus or by guiding a precision weapon to its target. Digital age warfare completely fits with Sun Tzu's observation that "war is such that the supreme consideration is speed."[333]

In terms of information age *shi*, a Trojan Horse virus in a computer could represent "potential" or a strategic advantage. A Trojan Horse is a virus that "is a form of malware that appears to perform a desirable function but in fact performs undisclosed malicious functions that allow unauthorized access to the host machine."[334] If a hacker can gain access to a server through a backdoor and insert a Trojan Horse, and execute it at a time of his or her choosing, then the virus contains the characteristics of a drawn bow, sitting there and awaiting the release of potential energy to attain strategic advantage.

Civilian and military hackers attempt to exploit the disposition and strategic advantage that electrons create. These activities are difficult to trace directly to the PLA or to government authorities due to the anonymous character of the Internet. This situation of anonymity adds to the *shi* or strategic advantage of the hacker. Further, the hacker uses packets of electrons as stratagems to change strategic advantage into a force or power to use against an opponent. That is, a packet of electrons can execute a stratagem such as "rustle the grass to startle the snake" (cause firewalls to alert and thus expose defenses when probed).

There are also some very specific applications of *shi* to the PLA's experience. One such reference was an article on the strategic use of electrons in China's *Jiefangjun Bao*. The article noted that if form is the foundation and prerequisite for *shi*, then *shi* also holds and directs form. The authors added "not only should network warfare power be flexibly combined at a specific time and space, its use must be delayed for the best moment to attack or defend."[335]

The utility of *shi* is applicable to a state's capability to execute and conduct strategic network warfare. Network warfare cannot exclude strategies and even has a higher requirement for them, according to the authors. Force capability involves the strength or weakness to control the direction and flow of information; the amount of data possessed by combatants; the degree of network architecture redundancy and the speed of recovery after being attacked; the different combat objectives of forces with different powers; and the adaptation to a corresponding military strategy to attack, defend, hide, or move. Successfully mastering these elements can manifest itself as one's strategic advantage.

Retired General Tao addressed the intangibles of *shi*. He wrote that a commander must make use of advantageous terrain, seize upon favorable opportunities for fighting, and have superiority in the quality of troops.[336] Put in terms of the information age, this would indicate that troops must understand the terrain of the computer, seize opportunities where they exist, such as in reconnaissance of networks (thereby setting

333 Ibid., p. xxiii.

334 Trojan Horse, *Wikipedia*, accessed 16 January 2009.

335 Liu Wanxin, Dang Wanlong, and Zhang Dan, "Network Attack and Protection Also Need Strategies," *Jiefangjun Bao*, 2 January 2008, p. 6.

336 Tao, p. 130.

the stage to win the fight before the first battle), and train information technology professionals. It is also important to maintain a morale advantage, which the Chinese feel they have accomplished through the renovation of their political system to now include media, legal, and psychological warfare types. A morale (cultural) advantage can also be created or exploited when one works in the absence of any defining international cyber laws.

The transformation of the PLA from a mechanized to an information-ized force fits the criteria of trying to turn a situation to its advantage. Of concern to Western societies should be the question of whether "shaping the situation" (as the US linguistically understands preemptive moves), from the Chinese perspective, now could involve controlling market societies and manipulating the electronic flows of free societies. Can one well placed and educated computer specialist serve this purpose today and stop the flow of ten thousand (or more) decisions in the market place? General Tao notes that in China there is the saying: "With only one man guarding the mountain pass, ten thousand men are not able to pass."[337]

War Control

Another concept that the Chinese are discussing during their transformative military shift from mechanization to informationization is war control. War control refers to the guidance and management of a war effort. This term is not familiar to many Western theorists, since the terms "crisis management," "command and control," "superiority," and "shaping" dominate their doctrinal discussions. There are similarities between some of these US concepts and China's concept of control. For example, the intent and implied use of a Western term such as shaping is actually to impose the ability to control a process or activity of some type.

Another definition of war control is located at the website www.laocanmou.net, a military website located in Lanzhou. It defined war control as "the political director of war, the occurrence, development, scale, intensity, and consequences of deliberate acts of imposing restrictions and constraints."[338] War control is defined in the 2001 book *The Science of Military Strategy* as the war conductor's behavior to limit and consciously restrain the occurrence, development, scale, intensity, and outcome of war.[339] The two definitions are nearly identical, meaning the definition has not changed much over the past several years. The Lanzhou definition was accessed in 2010.

War control involves preventing war, controlling its occurrence, controlling its vertical and horizontal escalation, and striving to reduce the consequences of war. National interests guide the development and control of military strength. The selection of war means must correspond with the object of interest to be obtained, and

337 Tao, p. 128.

338 Website and translation provided to the author by Mr. Scott Henderson, FMSO, on 10 November 2009.

339 Peng Guangqian and Yao Youzhi, *The Science of Military Strategy*, Military Science Publishing House, 2005. The section on war control was reprinted as an article in the journal *China Military Science*. See "War Control," *China Military Science*, No. 6 2005 (in English), pp. 129-141.

war's conductors should adjust military strategy according to the national interests at stake.[340]

Arms control, crisis control, and armed conflict control are all components of war control.[341] Arms control is divided into vertical arms control and horizontal arms control, with the former aimed at limiting or reducing the scope of military potential and the latter aimed at limiting the proliferation of certain weapons.[342] Crisis control is the control of the tense political and military situations caused by intensified contradictions of national interests. One must strive to remove the negative factors leading to a crisis. A crisis is a dynamic process, and it includes the stages of inception, escalation, de-escalation, and termination. The measures for crisis control and management are confidence building (measures to prevent the emergence of a crisis), increased transparency, enhanced personnel exchanges and contacts, joint disarmament and arms control, the establishment of regulations, and the creation of supervisory organizations.[343] To control a crisis one must find the intersection of interests, compromise appropriately, and strive for benefit for both sides; keep uninterrupted communications; and adopt coercive measures to prevent negative influences (weapon embargos, economic sanctions, and military blockades).[344] The control of armed conflict includes the control of its aim, means, targets, methods, duration, and space.[345] If cyber topics are under discussion for each of these control issues, they (cyber arms control, cyber crisis control, or cyber armed conflict control) will be elevated to a spot of extreme importance.

Preparatory activities are necessary for imposing war control. These activities include: scientific predictions on the prospects for war or crises, plans to cope with crises and contingencies, the preparation of military strength, and the improvement of non-military means. However, these activities also include reconnaissance. Reconnaissance lays the groundwork for achieving future results and aids in the development and analysis of war control issues.[346]

The Chinese have been studying the concept of war control for several years. Evidence of this is a 2002 National Defense University Press book titled *War Control*. Author Xiao Tianliang listed seven parts to the book:

- The theory of war control
- The control of history and the heritage of war
- Controlling conditions in time of war
- Mediating war
- Correctly handling and controlling crises
- The flexible and appropriate use of the means of warfare

340 Peng and Yao, p. 209.
341 Ibid., p. 197.
342 Ibid., pp. 199-200.
343 Ibid., pp. 202-204.
344 Ibid., pp. 205-206.
345 Ibid., pp. 207-208.
346 "War Control," *China Military Science*, No. 6 2005 (in English), p. 140.

- The use of war control in China's future.[347]

The journal *China Military Science* offered an interesting article on war control and informationization in 2010. Authors Zhang Yu, an associate professor at the Shijiazhuang Army Command Academy, and Academy lecturers Liu Sihai and Xia Chengxiao stated that a "post-emptive" move is "not an effective way to seize the initiative on the informatized battlefield."[348] To seize the initiative and control war in the initial state of conflict, the active offense must be emphasized. That is, when signs of enemy invasion are clear, then China should seize "early moments of opportunities to dominate the enemy"[349] through offensive operations which cannot be separated from active defense. Guidelines offered for controlling war include establishing favorable conditions in the opening of war, placing equal emphasis on deterrence and combat, grasping the center of gravity of war, destroying and attacking systems, strengthening the interactions between combat systems and war systems, and ending war as early as possible by combining fighting with negotiations.[350]

Peng Guangqian and Yao Youzhi, the editors of *The Science of Military Strategy*, write that the essence of war control is the strategic conductor's initiative. The strategic conductor must give play to his subjective initiative and carry out correctly the strategic guidance required to prevent the occurrence of crises and the escalation of a conflict. Only in this way can the objective of war control be attained. National interests are the guiding element in war control and strategic conductors must grasp national interests in a fundamental, long-term sense. These interests control military strength and the war means to be used.[351] Thus, it should be of interest to US analysts to uncover the objectives of China's cyber espionage initiatives and the subjective initiatives behind them.

Externally, war control involves observing and applying international law. Any strategic war control conductor must take these laws into consideration in his planning process.[352] Here the Chinese have learned to operate in uncharted waters. The near total absence of international law for cyberspace has offered them a blank playing field where anything goes in the cyber espionage arena.

Internally, the Chinese have instituted strict control laws. The State Internet Information Office will initiate war control at the local level. Among other duties, it is the organization responsible for directing the development of online gaming, online video, and online publication industries; and for assigning the duties to investigate and punish websites violating laws and regulations. It will also oversee telecom service providers in their efforts to improve the management of registration of domain names, distribution of IP addresses, registration of websites, and Internet access.

347 Book description found at www.bi3jia.com, accessed 10 November 2009.

348 Zhang Yu, Liu Sihai, and Xia Chengxiao, "On the Art of Controlling War Situation in Informatized Warfare," *China Military Science*, No. 2 2010, pp. 24-31.

349 Ibid.

350 Ibid.

351 "War Control," p. 139.

352 Ibid., p. 141.

War Control Discussion at an Art of War Symposium

At the 2009 Chinese symposium on Sun Tzu's *Art of War* held in Beijing, one of the symposium's breakout groups was devoted to the topic of "war control." Several opinions were offered. First, a Taiwanese spokesman stated that there were three aspects of war control: preventing war, controlling the scale and depth of a war, and reducing risk after war breaks out. He focused his attention thereafter on the prevention aspect, noting that prevention has three aspects. The first is the control of "slope theory" or the ability to keep war from sliding into an abyss from which no one can escape. Sometimes third parties on the fringe are needed to stop two other parties from sliding down a slippery war slope. A second aspect is constructing a smooth channel of information so that communication is never cut off. If a channel of communication or information is cut off, then miscalculations will result. Finally, when a party feels threatened or stepped upon, there must be a correct way to find a channel for an outlet to express this perceived misrepresentation of justice. If not, then war will occur. The Taiwanese representative felt this is what occurred on 9/11 with Bin Laden, that he had no other recourse or outlet to express his rage. Most Americans would obviously disagree with this assessment.[353] In the cyber age China is on its own slippery slope with all of the worldwide hacking activities in which it has been and still is engaged.

A Chinese military officer from the Academy of Military Science at the Sun Tzu symposium offered three phases to war control: preventing or dissolving a crisis, controlling the war process (that is, its magnitude and scale), and controlling a war's outcome. Subordinate tasks include controlling a conflict's escalation and controlling miscalculations.[354]

War Engineering—The Information-Age Version of War Control?

There is another concept under consideration by the Chinese military that is similar to war control, the concept of war engineering. Major General Hu Xiaofeng, a professor in the Information Operations and Command Training-Teaching and Research Department at China's National Defense University, noted that the age of informatization requires new approaches to the study and management of information-age wars. War engineering is one of these new approaches.[355]

War engineering arose, Hu contends, from the requirement to find a method to study, manage, and control information-age war systems. Chinese war engineering is "a method of systems engineering that studies, designs, tests, controls, and evaluates war systems and that is guided by systematic thinking, based on information technology."[356] The most important element of war engineering is to maintain control of war systems. Through war systems, control of the course of operations is possible.[357] The concept is

353 Author's notes from the symposium.

354 Ibid.

355 Hu Xiaofeng, "On War Projects" or "The Basics of War Engineering," *China Military Science*, No. 3 2007, pp.13-21.

356 Ibid.

357 Ibid.

centered on managing warfare and has total victory as its goal.

War engineering looks at combat as a nonlinear, complex adaptive system. War engineering studies, designs, and manages war requirements, theories, experiments, and processes. It has five parts: requirements, planning, testing, control, and evaluation engineering. Control engineering, the most important element, consists of strategic, campaign, and tactical command information systems which monitor situations, control decision-making, handle anomalies, and evaluate results.[358]

Hu concludes his thoughts on war engineering by quoting Engels, who noted that "it wasn't the inventors of new material measures; it was the first person who, in the correct manner, used a new measure that had already been invented." Hu believes China is searching for a way to be the first to use US information-age inventions to its benefit and prove Engels correct. China hopes to be able to manage and control war instead of reacting to it and to make wartime changes in advance (through simulations) instead of making changes as war requires or demands. War engineering, according to Hu, will be one of several catalysts that promote the further development of information warfare studies as China transforms its military from a mechanized to an informatized force.[359]

The term war engineering was brought to the attention of the Sun Tzu Symposium's (mentioned earlier) war control panel and its moderator. The Chinese participants were asked if war engineering and war control were the same thing. The moderator stated that not much importance should be attributed to the term war engineering, since it appeared in the journal *China Military Science*. The journal, he noted, is a place for new ideas and not policy. However, the discussion of the term indicates that war engineering and war control may be two ideas cut from the same cloth.

Cyber Control during the Jasmine Revolution

Scott Henderson, formerly of the US Army's Foreign Military Studies Office, has postulated, with sufficient evidence, that China's so-called Jasmine Revolution can serve as a case study of cyber control, albeit not war control. The Jasmine Revolution was the name given to online movements in China that appeared to be a citizenry response to the Middle East's Arab Spring events. Chinese authorities were clearly threatened by these pro-democracy incidents. They censored the word Jasmine from social networking sites, as well as from China Mobile (a state-owned leading telecommunication company that provides mobile voice and multimedia services) and China Unicom (a state-owned telecommunications operator).

Street protests, somewhat limited in numbers, started on 20 February 2011 in Beijing, Shanghai, and several other locations in China. Plain-clothes security officers quickly thwarted these actions, to include beating several foreign journalists. China's security forces had practiced their actions against protesters in the past when they confronted Falungong, Free Tibet, and pro-democracy Hong Kong supporters, all of whom also utilized cyber links to generate support.

358 Ibid.

359 Ibid.

Mr. Henderson breaks the control mechanisms that security forces used into two aspects: passive defense and active defense. Passive defensive actions had three phases. The first involved blocking (Chinese authorities blocked the Chinese word for "Egypt" as a search term on 29 January); the second involved internal monitoring of numerous sites, especially those associated with the protest movement; and the third involved external monitoring (on 17 December 2010 China began online blocking tactics against outside revolutions taking place in Tunisia and Egypt). Active defensive measures were broken into four aspects: intimidation (blogger Stoney Wang from Shanghai described his version of forced interrogation designed to intimidate him); campaigning (high ranking public officials make public statements to dissuade protesters); self-censorship (based on the circulation of directives from State Council offices); and attacks (hackers launching distributed denial of service attacks against specific sites).[360] The overall effect of these passive and active measures is to exert actual or implied cyber control over the activities of social networks and their netizens.

A government follow-up on the Jasmine Revolution has witnessed a set of new types of cyber controls. Loretta Chao and Brian Spegele, reporting from China for the *Wall Street Journal* in December 2011, wrote that to defend Chinese cyberspace from "harmful information" authorities announced rules to require users posting microblogs to register "their real names with the microblogging services."[361] These will be verified by government authorities and thus eliminate anonymity. The rules also ban posts that "spur ethnic resentment, discrimination, or rallies 'that disrupt social order.'"[362] The Chinese authorities have worried about the growing influence of microbloggers to report on accidents, protests, and safety issues around the country that, in turn, generate protests and demands for better service.

Conclusion

Chinese information operations are a curious mixture of Western and Oriental thought. While claiming to represent informatized thought based on Chinese characteristics, Western theory continues to influence Chinese work. For example, Chapter Nine of this book on system of systems thinking, a concept that originated in the US, represents a concept the Chinese appear to have made a center-piece of their future operational planning. The difficulty, then, is finding the real essence of Chinese informatized thought.

The three concepts discussed above (*shi*, war control, war engineering) are representative of how China's is attempting to blaze its own path by relying on traditional concepts. Western analysts rarely, if ever, discuss *shi*. It is an Oriental concept. However, Western sources will discuss courses of action or shaping an environment, two ideas that come close to both *shi* and to the meaning of control.

360 Author's discussion with Mr. Henderson, December 2011.

361 Loretta Chao and Brian Spegele, "Beijing Tightens Cyber Controls," *The Wall Street Journal*, 17-18 December 2011, pp. A1, A11.

362 Ibid., A1.

China's focus on virtual *shi*, or efforts to attain a strategic advantage in the cyber world, and on information control, which is working hard to surpass information superiority in importance, are keys to understanding Chinese reconnaissance efforts. If one is able to attain strategic advantage through planting Trojan horses or viruses or spotting vulnerabilities in Western systems via reconnaissance activities, then it is possible to "win victory before the first battle." That is, planting destructive codes that can be activated at a time of China's choosing; or knowing a system's weakness ahead of time helps attain the initiative in future battles. Sometime reconnaissance efforts are assisted through cognitive attacks, such as controlling or manipulating the information a source receives, which could cause the source to divulge important information. It is no secret that the Chinese have conducted extensive reconnaissance activities of US and UK systems, among other nations', over the past several years. Google, the Pentagon, and other key facilities have all been penetrated.

The subtle shift in emphasis concerning the concept of information superiority toward information control is related to *shi*. To attain a strategic advantage, control in some nature over a situation is usually required. Originally known as the pinnacle of the battlefield struggle and the way to achieve other levels of dominance (airpower, naval, space, etc.),[363] several noted Chinese theorists have thoroughly reexamined the information superiority concept. The main reason for this shift is understandable. Chinese strategists want to define information superiority for themselves and not rely on foreign concepts. They also realize that information superiority, while important, can be an illusion if not properly understood. For example, a force may think it has total superiority if friendly systems are collecting all information and preventing the collection of information on friendly systems by an adversary. However, collection alone does not guarantee information superiority, and that is where the illusion arises. If friendly superior systems are collecting selected or fake information, then analysts and, consequently, decision-makers do not really have dominance or superiority. They have what might be termed information inferiority, which could lead to an adversary dominating friendly forces. They have surrendered control for superiority. Further, information superiority is a dynamic concept that can shift back and forth once battle begins, depending on each side's prudent actions.

In 2007 Dai Qingmin, the former director of the PLA General Staff's Fourth Department, which is responsible for information operations, wrote that information operations refer to a series of operational actions undertaken to gain and maintain information superiority on the battlefield or control over information.[364] Dai makes it appear that superiority and control have become somewhat synonymous and an either/or proposition.

As the PLA attempts to develop an information-style strategic advantage, the West would be wise to watch developments in the PLA and its efforts to create an asymmetric

363 Peng Guangqian and Yao Youzhi, *The Science of Military Strategy*, Military Science Publishing House, 2005, pp. 153-156.

364 Xu Genchu and Dai Qingmin, *Study Guide for Information Operations Theory*, Academy of Military Science Press, November 2005, pp. 70-71.

situation in information confrontations, thereby gaining relative information superiority, "increasing its bargaining chips for victory in paralyzing an adversary's command and control system and tearing apart the adversary's operational system."[365]

Successful electronic reconnaissance activities enable the PLA to put into place the initial stages of its war control planning process. War engineering may be a way to control potential war or peacetime situations or to implement *shi*. Western analysts must become aware of the purpose behind these Chinese reconnaissance activities if they hope to remain the lead force in twenty-first century cyber prowess.

365 Zhao Xiaosong and Wei Yudu, *The Theory of Military Information Superiority*, Beijing National Defense University Publishing House, 2008, p. 441.

PART THREE
CYBER ATTACK PLANNER

CHAPTER SEVEN
THE INFORMATION OFFENSIVE VERSUS ACTIVE DEFENSE IN CHINESE INFORMATIZATION THEORY

Introduction

Between 2009, when this author's last book *The Dragon's Quantum Leap* was published, and 2011, the Chinese produced numerous books and countless articles on cyber or information-related topics under military supervision. Highlights of the few books and numerous articles that FMSO was able to obtain are presented below. The main themes included offensive activities, control of information and the Internet, reactions to the Stuxnet virus, information superiority (IS) definitions, local war and operational guidance under informatized conditions, strategy, and core military capabilities in the information-age. The two books reviewed below are 2008 publications obtained in 2011. The interesting theme in many of these works was the continued emphasis on information offensive activities.

Articles and White Papers on Information Topics 2010-2011

On the Art of Controlling Situations in Informatized War, 2010

Zhang Yu, Liu Sihai, and Xia Chengxiao wrote one of the most interesting articles that stressed Chinese offensive information activities. The authors stated that control over war situations includes both objective and subjective factors. Objective material factors include high-tech reconnaissance devices, command and control measures, and precision-guided weaponry, which are mechanisms that allow for quick analysis and response. These conditions cannot be separated from the subjective efforts of the war commander's efforts to flexibly use the art of controlling war situations. This "art" includes the use of stratagems. The PLA's military strength is increased when "fighting skillfully with superior art of stratagem in the guidance of controlling war situations."[366] As the PLA attempts to close the gap between quantitative and qualitative objective conditions, it must utilize subjective guidance to create conditions for controlling war situations. The selection of center of gravity targets is dependent on a serious analysis "of the main contradictions in the system of systems confrontation between us and our enemy."[367] After a center of gravity has been struck, the PLA must watch for signs of shifts in the center of gravity, which often occur. Here the work of reflective strategists is key.[368]

Control over war situations requires that information dominance be seized and the initiative on the battlefield won. While the authors insist on the strategy of post-

366 Zhang Yu, Liu Sihai, and Xia Chengxiao, "On the Art of Controlling War Situations in Informatized Warfare," *China Military Science*, No. 2 2010, pp. 24-31.

367 Ibid.

368 Ibid.

emptive moves, they hedge on the point noting that:

> While post-emptive moves are a self-defensive strategy of defense upon which our military must insist in the opening of war, it is not an effective way to seize the initiative on the informatized battlefield. To achieve the goal of seizing the initiative, the art of controlling war situations in the initial stage of combat must emphasize active offense, striving to dominate the enemy by capturing early moments of opportunities and conquering the enemy in early battles.[369]

When signs of enemy offensive actions are clear, cross border operations should boldly strike against them. Thus, in the initial stages of future war, "our military's seizure of early moments of opportunities to dominate the enemy by conducting offensive operations cannot be separated from the basic requirements of active defense."[370] The focus must be on striking an opponent's critical links and vulnerabilities in order to control situations. A system's structure and organization are as important for control purposes as are the quantity of people or equipment.

Control extends beyond the battlefield since informatized war is a war of system of systems confrontations, and destroying systems is an effective way to control war situations and the war's course. Informatized war includes not only military but also political, diplomatic, and economic operations. Strategic adjustments are continuous. Since the objectives of war in the information age are becoming more limited, the relationship between politics and control over war situations is closer than before. This requires the close coordination of military and nonmilitary means.[371]

There are several guidelines for controlling war situations in inform-atized war: focus on establishing favorable conditions in the opening phase of war; place equal emphasis on deterrence and combat; focus on guiding war situations (through seizing knowledge via C4ISR systems); emphasize attacking and destroying systems; firmly grasp the center of gravity of war (described as the attainment of information dominance); make the best use of circumstances; focus on dealing with complicated situations; strengthen the interactions between combat and war systems; understand the changes that develop in war situations; respond quickly; make adjustments with flexibility; focus on ending the war quickly; combine fighting with negotiations; and end the war decisively on just grounds and with restraint.[372]

Main Forms of Local Warfare under Informatized Conditions, 2010

Dong Xuezhen and Ren Desheng discussed operational forms of warfare, described as the ways and means used by a main force to achieve wartime goals. Past operational forms of Chinese warfare include positional warfare, mobile warfare, and guerilla warfare. Today, the operational form of future local warfare under informatized

369 Ibid.
370 Ibid.
371 Ibid.
372 Ibid.

conditions must be added to this list. Actions have progressed from ground-based, close-range combat to include outer space, electromagnetic space, and online space, with the latter touching on mental space.[373]

The authors note that "our armed forces should use 'information warfare, firepower warfare, mobile warfare, and control warfare' as the main operational forms to win a local war under informatized conditions."[374] They add that the means (and main forms of operations) to achieve the goals of such a war include countermeasures of each type (information, firepower, maneuver, control). Information war refers to countermeasures against an opposing side in the areas of information acquisition, transmission, processing, and utilization. By target, these actions would be against intelligence countermeasures, network and electronic countermeasures, and psychological countermeasures. Making information warfare the main operational form of future war helps further the PLA's awareness of information warfare and enables it to build such forces more quickly.[375]

Firepower strikes are no longer all-area suppression oriented but rather focus on destroying specific points under informatized conditions. They enable a departure from personnel-based war to firepower-based war. Maneuver warfare is now joint and multidimensional. It attempts to impose absolute maneuver dominance to paralyze an opposing force and to capture key targets. Finally, control warfare is the final battle of the entire war. It includes control over the enemy in terms of time, space, information, and psychological conditions. It also includes searching for any remnants of enemy troops in order to ensure stability in the war zone. Control warfare can employ violent means, but more often than not, the authors add, it includes the following: sealing-off areas or blockades; guarding and patrols; media propaganda; information control, and psychological offensives.[376]

Operational Guidance under Informatized Conditions, 2010

This article listed ten dialectical (opposing) aspects of relations when planning operational guidance under informatized conditions. Doing so is important, from a Chinese perspective, since the dialectical grasp of opposite concepts helps direct future operations and enables victories in war. Neither of the elements of the pairs that follow can be totally eliminated. The important point to remember is that both of the opposites can apply, depending on the circumstances and their creative application. These opposing aspects were as follows:

- Relations between contact and noncontact operations;
- Relations between linear and nonlinear operations;
- Relations between regular and nonregular operations;
- Relations between hard strikes and soft kills;

373 Dong Xuezhen and Ren Desheng, "On the Main Operational Forms of Local Warfare under Informatized Conditions," *China Military Science*, No. 2 2010, pp. 15-23.

374 Ibid.

375 Ibid.

376 Ibid.

- Relations between decisive operations and protracted operations;
- Relations between battlefield transparency and the fog of war;
- Relations between full-spectrum superiority and partial superiority;
- Relations between technological gap and cost gap operations;
- Relations between dynamic energy concentration and force concentration;
- Relations between armament and natural environment[377]

Quoting Mao, the authors of the article note that "war is the competition of strength but strength may change from its original form in the course of war." Thus they warn that in all cases it is unwise to underestimate either element of the pairs of opposites. Take, for example, the authors' discussion of nonlinear and linear operations. Non-linear operations are defined as operational actions for delivering simultaneous strikes on important targets to the entire depth of the operational domain with long-range strike weapons according to the unified operational intent. The essence of nonlinear operations is all-dimensional joint operations. However, this does not mean that nonlinear operations will of necessity supersede linear operations which are still required in concrete battles. Or take regular and nonregular operations. The former refers to conventional battle methods. However, when flexible strategies or tactics are required nonregular methods will take precedence especially if two sides have huge asymmetric differences between them in terms of equipment, men, and organization.[378]

With regard to informatized war in particular, the authors expounded on several issues affected by information technology. Primary among those is the dilemma of transparency versus the fog of war. Without a doubt, battlefield transparency is enabled by information technology and it helps attain quick victories. However, the fog of war can be a double-edged sword. Battlefield transparency can be used by an opponent to develop other fog-of-war conditions through the creative use of decoys and other means of deception described by the authors as "arranging many information mazes to mislead the enemy."[379] Further, battlefield transparency is conditional on the ability of an information system to operate. Once influence is denied or destroyed through targeted strikes it may be very hard to regain it in this continuous battle between the haves and the have-nots. Decisive victory is preferred over protracted methods of employment in informatized war, but protracted methods can still play a role.[380]

Thoughts on Strengthening the Informatization Building of Reserve Units, 2010

In order to continue to build information talent and capability in reserve units, Chairman Hu Jintao stressed the following points at the Communist Party of China's

377 Yang Baoming, Zhao Changjun, and Xu Jianhua, "Dialectical Considerations on Operational Guidance under Informatized Conditions," *China Military Science*, No. 4 2010, pp. 73-83.

378 Ibid.

379 Ibid.

380 Ibid.

17th National Congress: rely on science and technology to strengthen the PLA; make the PLA's strategic objective the building of informatized forces and winning informatized wars; integrate mechanized and informatized forces; conduct training under informatized conditions; build informatized logistics; cultivate new-type informatized personnel; and change the model of generating combat capabilities to have an informatized character. Training methods include online teaching, online command, online confrontations, and online assessments. The hope is that the PLA's system of systems operational mode will improve, as this concept is fundamental to the PLA's objective of informatization building.[381]

Analysis of Combat Styles in Informatized Warfare, 2011

Informatized weapons, combined with men's talents, produce combat power. It results in a combat style characterized by initiative, discipline, willpower, and creativity. One more element is added to combat power in informatized warfare, the system of systems operational capability.[382]

Combat styles are "the mental force and behavioral standard for implementing the strategic principles and operational concepts to fulfill the strategic, campaign, and combat intentions"[383] of commanders. They serve as the foundation for winning informatized warfare. The latter is characterized by its nonlinear, noncontact, and asymmetric forms. The goal of this combat style is to seize the initiative on the basis of respecting science and carrying out system of systems operations. Informatized war relies on using time and speed to increase one's efficiency in carrying out operational activities. Commanders must be able to engage in high-tech strategic planning; to respond agilely to unexpected changes; and to innovate when required.[384]

On Core Military Capabilities in the Information Age, 2011

Deterring war requires the core military capability of being able to win war. The author defines core military capabilities as "the actual support for winning local wars under informatized conditions and also the foundation and precondition of non-war military actions."[385] Winning such wars is a strategic objective of the PLA. Building core military capabilities involves building a system of systems infrastructure that is agile, high-speed, and strong. This involves the coupling of firepower and mobile capabilities with information capability. The key point is to paralyze an adversary's operational systems and not to outright destroy them. Another key is the seizure of decision-making and action superiority through information superiority.[386]

381 Zhao Xiuming and Yu Kezhen, "Thoughts on Strengthening Informatization Building of Reserve Units," *Guofang*, September 2010, pp. 55-56.

382 Shi Daoxiang, Wang Junxue, Li Qu, and Chen Shengwu, "Analysis of Combat Styles in Informatized Warfare," *China Military Science*, No. 2 2011, pp. 9-12.

383 Ibid.

384 Ibid.

385 Shen Genhua, "On Core Military Capabilities in the Information Age," *China Military Science*, No. 2 2011, pp. 44-53.

386 Ibid.

Offensive capabilities are now primary and defensive capabilities secondary. As the author notes:

> At present when the waves of informatization sweep across all social corners including the military domain, thanks to the realization of destruction upon discovery and operations outside defensive zones, the counterattack capability of the defensive side is substantially restricted and the offensive side has marked superiority. Thus the attacking capability will become a key factor in influencing the outcome of war.[387]

Informatized war patterns have established the dominant feature of offensive operations. The PLA's strategic notion must be to take the offense as the main form of operations. The integration of hard and soft kill capabilities will be required. Author Shen Genhua added that "deterrence will be effective only with the support of actual operations and may pale into insignificance without the support of actual operations."[388]

Years earlier other authors had also addressed the deterrence aspect of information technology. A *China Military Science* article in 2005 discussed "Systems of Military Strategy in the Information Age."[389] Military strategy was defined in several ways, but it was noted that "In the final analysis, military strategy is the guidance and utilization of innovative activities. The revolution in information technology has provided unprecedented conditions for substantial innovation."[390] The authors wrote that "seizing the initiative to control information and networks has become the prerequisite for conducting operations and the marker for achieving the initiative."[391] The authors add that war has evolved from material depletion of the industrial age to operational depletion of the information age, where the aim of networks is to control operational space.[392] This becomes the best strategic objective: to use information technology's deterrent function with the main goal being to position strategic objectives within the scope of national interests instead of seizing territory. Control of a situation allows for the quick transmission of orders and the correct orientation of forces toward the correct targets.[393]

The primary objective consists of paralyzing an opponent's strategic command systems to introduce the deterrence function. The five steps to this process are striking at an opponent's strategic command system, their economic foundations, that nation's transportation infrastructure, the human resources of the country (especially reserve

---

387 Ibid.

388 Ibid.

389 Zhang Feng, Liu Zengliang, and Lu Dehong, "Systems of Military Strategy in the Information Age," *China Military Science*, No. 2 2005, pp. 90-99.

390 Ibid., p. 98.

391 Ibid., p. 91.

392 Ibid., p. 93.

393 Ibid., pp. 95-96.

personnel), and the armed strength of the country in question.[394] No longer is the geographical axis the focus of attention, but rather the focus becomes a determination of the configuration of the enemy's "core" and the selection of the right troops to attack key nodes.[395]

Further, psychological-cognitive warfare is now a most critical and direct form of operations; firepower is a means of achieving operational objectives of psychological-cognitive warfare. Network superiority works directly upon the core of the enemy's strategic heart, the will and cognition of the decision makers.[396]

China Considers Stuxnet

Even though the Stuxnet virus was first discovered in June 2010, it did not appear prominently in the Chinese press until September of that year. First reports were that this was a super cyber bug that had infected millions of computers in China and was designed to attack Siemens supervisory control and data systems. Russian cyber security specialist Eugene Kaspersky was quoted by the Chinese as stating that "we have now entered the age of cyber-warfare."[397]

Other reports were more dramatic. The Hong Kong-based *South China Morning Post* noted that the Siemens system is widely used in China at airports, railways, nuclear power plants, and at the Three Gorges Dam. This especially worried hydropower experts. The paper reported that the *Xinhua News Agency* had reported the day before that "nearly a thousand" industrial plants and facilities in China had been infected, with the source of the attacks being servers in the US.[398] A day later, in a 1 October report, the threat was downplayed as reporters considered it more limited and inconsequential. Apparently China's National Computer Virus Emergency Response Center did not even raise an alert over the virus. And an official at the Ministry of Industry and Information said it was aware of the virus's potential but would take no action until after the holiday.[399]

Chinese theorists are aware that the anonymity of cyberspace, the space-time element of attacks, and the flexible use of stratagems makes cyber reconnaissance or attack activities difficult to recognize and difficult to react against quickly. Further, these theorists note that cyber attacks such as Stuxnet are becoming more and more strategic and aimed at a country's infrastructure or at a society's willpower. With regard to Stuxnet, however, most of the reports were about infrastructure issues and the discussion continued well into 2011.

For example, in March National Defense University cyber warfare expert Li Daguang

394 Ibid., p. 91.

395 Ibid., p. 96.

396 Ibid., pp. 98-99.

397 Guo Qiang, "Web Superbug Seeking to Access China, *Global Times* Online (in English), 27 September 2010.

398 Stephen Chen, Stephan Finsterbusch, and Anita Lam," Cyber Worm Hits Mainland Industry," *South China Morning Post* Online (in English), 30 September 2010.

399 Stephen Chen and Stephan Finsterbusch, "Hackers Warn of Holiday Strike by Cyber Worm," *South China Morning Post* Online (in English), 1 October 2010.

(author of *Information System-Based Cyber Operations*) warned that Stuxnet was like opening a Pandora's Box, where the consequence of the action may far exceed people's control.[400] In June, authors Ye Zheng and Zhao Baoxian of the Academy of Military Science noted that the Stuxnet virus indicates the need for a network armament control system much like the nuclear armament control system of the past. The Stuxnet virus was the "first publicly reported virus directed against an industrial control system."[401] Further, the authors stated that China should establish "network borders" and "network sovereignty" as new concepts and principles. Network warfare, two analysts reported, has five operational forms: network intelligence, network paralysis, network defense, network psychology, and network-electromagnetic integration.[402]

The Chinese reports regarding the Stuxnet virus only blamed the US and Israel for the attacks. Siemens was not blamed by any of the analysts and commentators.

Books on Information-warfare Topics, 2008-2010

The Theory of Military Information Superiority

One Chinese work obtained in 2011 was Zhao Xiaosong and Wei Yudu's 2008 book, *The Theory of Military Information Superiority*. It is noteworthy for its interesting and wide-ranging views on Chinese definitions of information superiority. It represents one of the most comprehensive works on the topic. The authors cite several Chinese information technology experts and their definitions of information superiority, as well as the many characteristics associated with the concept.

The People's Liberation Army (PLA) appears to still be working on a final definition of IS due to the numerous definitions offered in the book and to the absence of an entry for IS in the Chinese work *Military Terms*.[403] As a result, considerable diversity remains in the understanding of this term. What follows are four truncated definitions of IS from books or articles by Lin Chunying and Li Chunhua; Dai Qingmin; Zeng Qingyang, and Zhang Dongmei and Wang Shengrong, which were cited in *The Theory of Military Information Superiority*:

> Possessing information supremacy first requires possessing information superiority. Information superiority in information warfare not only refers to having more information than the adversary, it also includes needing to possess stronger information acquisition, utilization, and control capabilities than the adversary…The amount of 'useful' information possessed is the primary indicator for measuring whether or not you have information superiority...Information control capabilities are also a key aspect reflecting

400 Li Daguang, "After One Opens 'Pandora's Box' of Cyber Warfare," *Jiefangjun Bao* Online, 10 March 2011, p. 12.

401 Ye Zheng and Zhao Baoxian, "How Do You Fight a Network War?" *Zhongguo Qingnian Bao* Online, 3 June 2011.

402 Ibid.

403 Zhao Xiaosong and Wei Yudu, *The Theory of Military Information Superiority*, Beijing National Defense University Publishing House, 2008, p. 433.

information superiority.[404] (Lin Chunying and Li Chunhua)

Information superiority refers to a kind of superiority when comparing the forces or postures of two antagonistic parties in an information struggle. The side in the superior position with regard to force or posture has information superiority; the side not in the superior position with regard to force or posture does not have information superiority, or is said to have information inferiority. Information superiority has implications regarding both force and posture. Superiority in the forces for information struggles can be divided into the two aspects of quantity and quality…Superiority in information struggles posture refers to the advantageous situation or pattern formed by information operations forces and weapons through their dispositions or actions.[405] (Dai Qingmin)

The so-called information superiority refers to one party's information security and overall capabilities for possessing and utilizing information being stronger than the other party's… Information superiority is primarily established in peacetime; in wartime it is a matter of unleashing it just before war. If it is not unleashed well it may similarly lead to a transposition of information superiority. And destroying the enemy's information resources really does not signify an increase in one's own information resources…The real significance of information superiority in combat lies in controlling the time initiative.[406] (Zeng Qingyang)

Information superiority refers to a conflict between two parties, with one party's information exploitation capabilities being stronger than the other party's. It is the result of a competition between the two parties' information exploitation capabilities, and includes the two aspects of static superiority and dynamic superiority. Static superiority refers to the extent of the information exploitation capabilities; it is acquired by building information exploitation systems and training information exploitation capabilities. Dynamic superiority (or information supremacy) refers to the dominant information posture that is acquired through information exploitation and information confrontation actions in war.[407] (Zhang Dongmei and Wang Shengrong)

Two Chinese authors, Jiang Fangran and Wang Changlin, discussed five areas of information superiority in *The Theory of Military Information Superiority*. They noted that a military must acquire information before the enemy (discover targets quickly and act before the enemy); have more information than the enemy (incomplete information

404 Ibid. See Lin Chunying, Li Chunhua, "Understanding Information Superiority," *Military Science* 1998, Volume 2.

405 Ibid., pp. 433-434. See Dai Qingmin, chief editor, *Introduction to Information Operations*, PLA Publishing House, November 1999, 1st Edition, p. 285.

406 Ibid., p. 434. See Zeng Qingyang, "A Few Thoughts on the Principles of Information Warfare," *China Military Science*, No. 6 2002, p. 59.

407 Zhang Dongmei and Wang Shengrong: "Theories and Guidance Related to Information Superiority," *Information Operations Research*, June 2005.

can result in loss of control); have higher quality information (must be true, relevant, and reliable); transmit information faster than the enemy (time between acquisition and action must be faster than that for the enemy); and have better information results than the enemy (exploit effectively).[408]

In another case in Zhao and Wei's work, three Chinese authors, Liu Liefeng, Song Zhizhao, and Chen Zhijun, further defined the concept, noting that information capabilities (measures that evolve and transform over time) serve as the basis for information superiority:

> Information superiority is a contest for superiority between the information capabilities of the red and blue sides. If the red side's information capabilities outweigh the blue side's information capabilities, then the red side has information superiority; on the other hand, if the blue side's information capabilities outweigh the red side's information capabilities, then the blue side has information superiority. Because of this, information superiority is a relative concept (a contest between the red and blue sides), and it can be expressed as follows:
>
> information superiority = red side's information capabilities/blue side's information capabilities
>
> …When information superiority is sufficiently large or when there is decisive information superiority, an absolute dominance of battlefield information is possessed, and information supremacy of battlefield information is possessed as well.[409]

The authors of *The Theory of Military Information Superiority* also cited the thoughts of Cao Xuefeng on information superiority. Cao wrote that two elements are necessary for military information superiority. They are:

> **Force.** Information force superiority mainly refers to one belligerent party having a greater degree of weapons informatization and the ability to acquire and process battlefield information, as well as the ability to attack and destroy the enemy's information systems that exceed those of the adversary. It includes the national information infrastructure, overall level of the military command and control system, advanced nature and defensive capabilities of battlefield information networks, quantities and qualities of information operations units and their weapons and equipment, appropriateness of the

408 Ibid., p. 435. See Jiang Fangran and Wang Changlin, "Five Standards of Information Superiority," *Liberation Army Daily*, January 31, 2004.

409 Ibid., p. 436. See Liu Liefeng, Song Zhizhao, and Chen Zhijun, "Three-Dimensional Quantitative Analysis of Information Capabilities," *Command, Control, and Simulation*, October 2006, Issue 5 Volume 28.

organizational system for informatized operations, the information qualities of personnel, and so on. However, this kind of force superiority is only a static comparison of both sides' operational forces; information supremacy is the outcome gained by a trial of strength on the battlefield. Because of this, a superiority of information forces alone will not necessarily be able to ensure the acquisition of information supremacy.

Posture. Information posture superiority mainly refers to the advantageous dispositions and patterns gained by information operations troops and weapons in their deployments and actions. This kind of superiority is closely related to advantageous material conditions, and it cannot be separated from the superiority of information force. At the same time, an advantageous posture cannot be separated from proper command and action during combat. Because of this, a superiority of information posture is a higher level of superiority than force superiority. If you want to be victorious in information operations, you have to create a certain degree of information posture superiority. Of course, having this kind of superiority only indicates that the conditions of the information struggles favor your side and that you are in a better situation than the adversary; this does not allow you to ensure control and mastery of the battlefield information initiative.[410]

These six ways of looking at IS offer a more comprehensive view of the topic than the US definition of IS, mainly because the US definition has been finalized and included in Joint Publication 1-02, *DOD Dictionary of Military and Related Terms*. There, IS is defined as follows: "The operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same." The Chinese definitions include several aspects of military strategy, such as achieving a correct information posture/strategic advantage (*shi*); establishing information superiority in peacetime ("win victory before the first battle") and unleashing it just before war; and achieving static (exploitation or reconnaissance, the prerequisite for information-age victory in Dai's opinion) superiority in peacetime before unleashing dynamic superiority in wartime.

Zhao and Wei write that high-quality military information, the prerequisite for acquiring information superiority, is measured by five criteria: reliability (credibility, authenticity, accuracy, etc.); timeliness (no lost opportunity, initiative, or victory); relevance (information for different user needs); completeness (all relevant information is included); and accuracy (precision). These criteria enable information superiority.[411] The authors add that "information superiority is a kind of description of the degree of information control," that is, the side with information superiority can control information without encountering significant resistance. Characteristics of information

410 Ibid., p. 439. See Cao Xuefeng, "Analysis of Two Elements of Information Superiority," *China National Defense News*, March 24, 2005.

411 Ibid., pp. 426-427.

superiority are that it is comprehensive and multifaceted, has operational relevance (since it must be turned into decision-making superiority and action superiority), has both gradual (built up during peacetime) and sudden (wielding capabilities in wartime) aspects of confrontation intensity, and can be dynamically acquired during a confrontation between spears and shields.[412]

Finally, authors Zhao and Wei write that for information to be effective its content must be of the highest quality (reliable, relevant, complete, and accurate); it must flow efficiently (be timely); and it must exploit its effectiveness (quality of the decisions made and the results after implementation). The authors then produced an IS diagram (see Figure One below) to demonstrate that information superiority can be achieved "only when one side surpasses the other in the three aspects of military information effectiveness":[413]

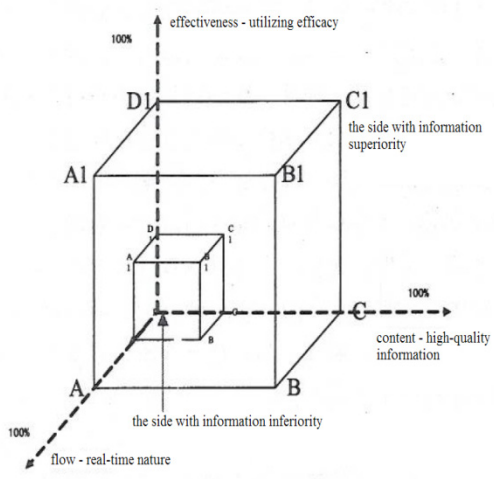


Figure One

Zhao and Wei also commented on the issues of knowledge and information and on the role of offense and defense as they pertain to IS. The authors noted that information and knowledge are the most important strategic resources in the information age; that the acceleration of information capabilities is a strategic choice that nations must make; and that gaining IS provides an assurance for winning informatized wars.[414]

To attain IS it is necessary to develop "attack and defense measures in the military information domain."[415] This requires "developing systemized information warfare offensive forces as the core…"[416] Attack measures must be systematic, comprehensive, and diverse. They must be capable of delivery at multiple times in multiple dimensions. This requires optimizing the integration of combat command systems and increasing

412 Ibid., p. 429.
413 Ibid., p. 438.
414 Ibid., p. 537.
415 Ibid.
416 Ibid.

the organization and proportion of military information offensive forces.[417] IS requires the continuous buildup of electronic warfare (EW) forces, the prompt establishment of new information operations units with computers and other new-concept weapons, and the establishment of a sound mobilization mechanism. Local resources have to be trained and organized in advance in order to make them into a powerful reserve force for information operations.[418]

These forces would be composed of five elements: electromagnetic jamming and suppression; computer network attacks; comprehensive firepower destruction; new-concept weapons (for example, electromagnetic pulse bombs, directed-energy weapons, and carbon fiber shells); and Special Forces sabotage (via disguise and infiltration or advance placement). Information defense requires strengthening the management of information and its security; the defense of key military information nodes (to include the camouflage of nodes and their spatial distribution); the improvement of counters to information jamming; and the strengthening of network security.[419]

New Perspectives on War

Another interesting book was Major General (retired) Dai Qingmin's 2008 work, *New Perspectives on War*, obtained in 2011. Dai previously served as the department head of the General Staff Department's Fourth Department, now designated as the Information Technology Department. Dai's book is rich in information, especially about integrated network-electronic warfare (INEW), his specialty.

Dai writes that in the information-age, warfare has moved deeper into the cognitive and social domains. These domains are now a focus for overall strategic planning and have resulted in influencing the political department's concept known as the three warfares (psychological, legal, and public opinion warfare, also described as the strategic means for achieving war objectives).[420] Another influence was US actions in the battle over Kosovo, wherein, according to Dai, all three forms of warfare were used. Information firepower on the cognitive and social domains resulted in "controlling strategy, driving campaigns, and coordinating tactics."[421]

A section of Dai's book is on "attacking combat systems." Dai explains that the "inherent nature of informatized operations is systems confrontation, and the heart of the informatized battlefield is integrated information support systems."[422] The value of information warfare, then, is as follows:

> Information warfare is a form of operations specifically directed at information systems; it is the nemesis of information systems. Even though firepower, especially informatized firepower, can also be used to attack information

417 Ibid., pp. 537-538.
418 Ibid., p. 538.
419 Ibid., p. 539.
420 Dai Qingmin, *New Perspectives on War*, PLA Publishing House, 2008, p. 64.
421 Ibid., p. 65.
422 Ibid., p. 98.

systems, information warfare can completely destroy information systems; it is highly controllable, very cost effective, and without a doubt is the most unique attack measure of the information age.[423]

Dai adds that, in order to paralyze a command and control system and lower its effectiveness and combat capabilities, it is necessary to conduct an information attack against an enemy's financial, transportation, telecommunications, and power systems.[424] It is not known if this represents a specified order of attack or whether it is just random thoughts from Dai.

Dai adds that information warfare measures can have a deterrent effect and can adapt to the requirement for controlling information-age wars. The use of EW measures, when considered as a force multiplier coefficient (the ratio of personnel needed when EW is not used compared to those involved when EW is used) was nine or higher when EW was used. When a variety of EW measures are used, the coefficient increases exponentially.[425]

Dai then describes battlefield network warfare, EW, and network warfare. Battlefield network warfare is "operational actions targeted against computer networks within a specific battlefield domain."[426]

EW emphasizes "attacks at the signals level and using intense electromagnetic capabilities to drown out target signals."[427] Network warfare "focuses more on attacks at the information level and inputting information flows with harmful functions into the enemy's computer network systems to achieve attack objectives."[428] Future combat will be "confrontations between the combat systems of the two belligerent parties. Confrontation against information systems that have already formed complete systems will be possible only by conducting integrated network and electronic warfare (INEW)…"[429]

Dai notes that his INEW concept, which uses EW to destroy an enemy's transmission of information and network warfare to destroy an enemy's capability of processing and utilizing information, destroys an enemy's ability to share and use information and offers a strong counter to network-centric warfare.[430] Information systems are the operational objectives of the INEW concept. The main support for network-centric war, in Dai's opinion, is the Global Information Grid (GIG).[431] Thus, the network-centric concept and the GIG are likely targets of a Chinese attack.

The overall objective for the buildup of China's military is to ensure that the transformation is revolutionary, modern, and standardized. The goal is to move

423 Ibid.
424 Ibid., p. 99.
425 Ibid., p. 100.
426 Ibid., p. 101.
427 Ibid.
428 Ibid.
429 Ibid., p. 102.
430 Ibid., p. 103.
431 Ibid., p. 106.

military transformation in the direction of higher unity, which includes uniting and safeguarding national security interests with national development interests. The strategic objective is to prepare to "build an informatized military and fight and win informatized wars."[432]

Conclusion

This chapter covered some of the developments in China's informati-zation theory over the past four years, with two books from 2008 and several articles from 2010 and 2011 providing the heart of the discussion. The focus was the increasing emphasis in the PLA on offensive cyber activities.

The 2009-2011 articles highlighted in this chapter stressed that China can no longer be intent on "post-emptive" moves in the cyber age and that key decision-makers may conduct offensive operations when "intent" is detected in an adversary's activities; that offensive operations cannot be separated from the basic requirements of active defense; that defensive counterattacks have been restricted and that today the offensive side has marked superiority; that a primary objective is to paralyze an opponent's strategic command system to introduce deterrence options; that controlling war in the initial stage of conflict must emphasize active offense; and that a system of systems infrastructure capability that can paralyze an adversary's operational system must be developed.

Two books were discussed. *The Theory of Military Information Superiority* demonstrated two things: that a definition for information superiority is still apparently under discussion; and that there are definite plans underway for conducting both offensive and defensive actions on the cyber battlefield. The book's discussion of IS demonstrated that authors interpreted the term differently. Elements that stood out included the following:

- To achieve IS one needs to possess stronger information acquisition, utilization, and control capabilities than the adversary;
- IS has two aspects, quantity and quality;
- IS is established in peacetime. It is unleashed just before war;
- IS's real significance lies in controlling the "time initiative";
- IS refers to a conflict between two parties, with one's exploitation capabilities stronger than the other's;
- IS as an equation is represented by the friendly side's information capabilities divided by the blue side's information capabilities;
- IS means having a greater degree of weapons informatization, a greater ability to acquire and process information, and a greater ability to attack and destroy an opponent than the abilities possessed by an adversary;
- IS is a higher level of superiority than force superiority.

432 Ibid., p. 184.

Developing information warfare offensive forces as a core component was stressed. These forces must be capable of delivery at multiple times in multiple dimensions, requiring the increased organization and proportion of information offensive forces.

Retired General Dai Qingmin's book, *New Perspectives on War*, emphasized the importance of the integrated network-electronic warfare concept he developed as a counter to defeat the network-centric warfare concept. Further, information attacks must be conducted against financial, transportation, telecommunications and power systems of an adversary if command and control systems are to be lowered in their effectiveness. Dai also noted that the GIG would be a likely target in wartime.

Several years ago Wang Yungming, writing in *Campaign Stratagems*, noted that high technology developments such as precision-guided weapons, global-positioning systems, electromagnetic decoys, technologically advanced camouflage means, and advanced night vision equipment can be used to produce illusions (both real and virtual) and thus impact the development and use of campaign stratagems. New battles of wits and improved wisdom and strategies are thus on the horizon. The soul of these revolutionary changes lies in the PLA's ability to innovate and apply information-based creative thinking. These material developments induce change and result in new means to apply strategy.[433]

It is clear that the PLA is continuing to innovate and expand its capabilities in the cyber arena, especially in regard to offensive thinking. To put offensive systems into action, commanders need high-tech quality personnel who, in the words of the Chinese, must also understand the appropriate level of stratagem utilization and its application to electrons. The focus on offensive cyber activities from 2009-2011 indicates that innovation in this area is ongoing and could be an area of focused development in the coming years.

433 Wang Yungming, "Campaign Strategy and Objective Conditions," in Zhang Xing Ye and Zhang Zhan Li, *Campaign Stratagems*, National Defense University, 2002, pp. 181-182.

CHAPTER EIGHT
CHINA'S BLUE FORCE

When "Blue Armies" are elite, "Red Armies" become strong.[434]

Significant progress has been made in building the "Informationized Blue Force" and battle laboratories.[435]

Introduction

During the 1970s Chinese delegations visited foreign army bases around the world. One of the things that interested them most was the development of opposing force (OPFOR) training. The Chinese delegations recognized that such training prepared Western armed forces for future war in a way vastly different from People's Liberation Army (PLA) training. The latter's training was only slightly creative, useful, and realistic.

Since 1980 there has been a significant push to improve OPFOR training in the PLA. This push eventually resulted in the creation of an OPFOR that is called the "Blue Force."[436] The Blue Force directly opposes the PLA Red Army in both simulations and actual training confrontations. All of the military regions are engaged in this type of training. An often stated metaphor is that the Blue Force is a "whetstone" on which the PLA can sharpen its swords and knives.

Recently, two Chinese journalists wrote that

> A 'Blue Force' is also called a notional enemy unit. A Blue Force shoulders the heavy mission of simulating a combat opponent in an exercise and thus improving combat power…they all wear blue arm bands and a distinctive badge on their chests which reads 'Blue Force.'[437]

This chapter will examine the evolving nature of China's Blue Force over the past ten years. The examination highlights several important aspects of the force's development,

434 Dia Feng and Ni Minzhi, "New Blue Armies Push Forward the Gradual Upgrade of Confrontational Training—Amphibious Blue Army, Informatized Blue Army, in Nanjing Military Region Accelerated Generation of More than 100 New Operational Methods, New Training Methods," *Jiefangjun Bao* Online, 18 July 2009, p. 1.

435 Full Text of White Paper on "China's National Defense in 2008," *Xinhua*, 0208 GMT 20 January 2009.

436 In Chinese writings, the words team, army, and force are used interchangeably to talk about an opposing force or OPFOR. This author has chosen to use the word "force" throughout when possible.

437 Hu Wei and Huang Jiandong, "Specialized 'Blue Force Brigade' in Decisive Battle on Exercise Ground," *Zhongguo Qingnian Bao* Online, 13 November 2009, as downloaded from http://zqb.cyol.com/content/2009-11/13/content_2934051.htm.

especially how it encourages initiative and thinking/acting like the enemy; and how it presents an informatized, high-tech opponent to the PLA.

Background

One source reports that the job of "Blue Team Commander" was created on 10 August 1980 in the Nanjing Military Region. At the time it was produced the model utilized training that was original and surprising. It forced Red Army commanders to use their intellect and brains to find answers to problems. In the past, commanders had been presented with preset problems that they could answer via rote memory from past experiences. Now no longer were PLA military exercises "stage performances" with the Red Army always victorious; the Blue Force was winning as much as the Red Force. Blue Force Commanders gathered foreign information, studied it, integrated it into training, and applied it flexibly. This converted "dead information" into "living enemy situations" and brought a commander's subjective qualities (that is, initiative and creativity) into play. PLA Red Force Commanders had to know Blue Force tactics and thinking, and they had to pit their wits against those of the Blue Force Commanders.[438]

The use of an information or cyber element appears to have emerged later. For example, one article on information warfare (IW) training in February 1999 described various teaching methods according to one's age. IW was defined as knowledge-style warfare, a special trial of strength between highly talented people. This definition arose from the fact that high-tech war demands a high level of knowledge by commanders and operators, strong psychological qualities, command ability, and operational skills. Recognizing that China lagged behind in several of these categories, the PLA leadership decided to carry out training at various levels. Each is age dependent. The first category is support-style talent, where the main targets are leading cadres who are over 40 years of age. These individuals are decision makers, and the aim is to eliminate their information illiteracy, to change their concepts through training (from mechanized concepts to simulated IW fighting), and to apply their new ideas to future war. The training content for this group is information technology basics, the theory of IW, and general knowledge of IW weapons. The training method is to focus on short training courses, supplemented by other methods.[439]

The second category listed in 1999 is transitional-style talent. Here, cadres aged 30-40 were targeted. As the future leaders of China, they must focus on enhancing their ability to command in IW environments. The training aims were to supply them with information- technology lessons they may have missed in college and to ensure they grasped the requirements, special features, and laws of future IW. It was also important for them to understand the components of information weapons systems and to have instructors lay a firm foundation for information theory. Finally, they must master the

438 Xiang Shouzhi, "How the Blue Team Commander Came to Be," *Jiefangjun Bao*, 26 February 2008, p. 9.

439 Zhang Zhenzhong and Chang Jianguo, "Train Talented People at Different Levels for Information Warfare," *Jiefangjun Bao*, 2 February 1999, p. 6.

principles, forms, methods, and skills for IW command.[440]

The third and final category is called regeneration-style talent. This involved cadres aged 30 or less. These individuals are already acclimated to an information society and possess a general, all-round foundation in modern information technology theory. Their focus is on both command and technology. They receive advanced IW training, from ideological concepts to a theoretical foundation to skill in application. They train for a longer period of time than the other two groups due to the breadth and depth of their instruction.[441]

The training for each age group includes:

- Basic theory, including computer basics and application, communications network technology, the information highway, and digitized units
- Electronic countermeasures and radar technology
- IW rules and regulations
- IW strategy and tactics
- Theater and strategic IW
- Information systems, including gathering, handling, disseminating, and using information
- Combat command, monitoring, decision making, and control systems
- Information weapons, including concepts, principles of soft and hard destruction, and how to apply these weapons
- Simulated IW, protection of information systems, computer virus attacks and counterattacks, and jamming and counter-jamming of communications networks.[442]

While this article made it appear that China is well on its way to developing a first-rate IW curriculum, later reports suggest that much work remained. For example, just two months later, in July 1999, a report noted the following:

> Irrationalities in the training content, system, and structure have kept IW training from truly becoming the mainstream of our military training. At present, IW training is in a "do-as-you-please" situation in which the content is not systematic, the operations lack order, there are no assessment standards, and management lacks regulations.[443]

The requirement to correct many of these shortcomings was reemphasized in October 1999 by Fu Quanyou, Chief of the Chinese General Staff at the time. He wrote

440 Ibid.

441 Ibid.

442 Ibid.

443 Sun Haicheng, Yang Jie, and Zhang Guoyu, "Let Information Warfare Training Rule the Training Sites: Practice and Reflections from the First All-Army Collective Training Session for Division and Brigade Chiefs of Staff in Information Warfare Theory," *Jiefangjun Bao*, 13 July 1999, p. 6.

that four new training aspects must be created. These were to create new IW theories, design a modern system of high-tech military training, create high-tech military training forms and methods, and create operational, coordinating, and support training management mechanisms.[444]

After initial resistance to the concept of a Blue Force, it soon became clear to those participating in the exercises that the Blue Force was an "instructor" from which many benefits could be attained. The Blue Force uses methods and procedures from many armed forces' experiences and not just those of the US. For example, in a recent exercise it was noted that a German World War II method was used to set up antitank obstacles.[445] Gradually the Blue Force took on high-tech missions that caused the Red Force to hurry up its transformation from a mechanized to an informatized force. In 2004, for example, the Beijing Military Region conducted an exercise where commanders studied "the characteristics of local wars under informatized conditions to build an informatized battlefield environment."[446] Literally hundreds of such informatized confrontation exercises have followed.

The Blue Forces serve as a laboratory for studying a potential opponent's future information warfare techniques, since Blue is purportedly equipped with the latest information technology gadgets, vehicles, and information-based thinking and doctrine. A Beijing Military Region unit noted that it had created a Blue Force not only to study the informatization of warfare, but also to get a lifelike opponent and to "think from somebody else's perspective."[447]

"Thinking from somebody else's perspective" has been a popular theme in China. For example, Wang Lin, Wang Yitao, and Wang Guibin wrote in 2005 about a method by which to better understand another culture or another's perspective. They wrote that subjects must avoid prejudice when studying other cultures and potential targets. One must actively utilize empathy toward another nation's cultural proclivities. To be truly empathetic, seven steps should be followed. These seven steps work in times of peace or war to get at a potential opponent's mind set. US Red Team instruction at the University of Foreign and Military Studies, located at Fort Leavenworth, Kansas and directed by Colonel (retired) Gregory Fontenot, follows a similar, though not exact, line of reasoning. The seven Chinese steps are:

- One must share the inner state of someone and recreate that person's inner image.
- One must recognize the types of cultural diversity in society.
- One must know oneself and individuals in a given culture.
- One must eliminate one's own isolation from the environment.

444 Mao Xiaochun and Chen Hui, "Chief of Staff Fu Quanyuou on High-tech Military Training," *Xinhua Domestic Service*, 0240 GMT, 16 October 1999.

445 Hu and Huang.

446 Zhang Kunping, Tian Jun, and Hao Mingli, "Xie Yong, Commander of the Combined Tactical Training Base under the Beijing Military Region on Base-Centered Real Troop Confrontational Drills," *Junshi Wenzhai*, 5 September 2004, pp. 8-11.

447 Ibid.

- One must take on the other person's perspective and thinking.
- One must acquire experience through empathy obtained from the five steps above.
- One must restore his or her inner state and re-experience one's own cultural state again. [448]

In addition to these cultural issues, the creation of a Blue Force required the acquisition of intelligent, informatized, and knowledgeable servicemen who could operate technical equipment and build a unit that truly represented a Blue Force. Some Chinese journalists believe the PLA has created a force that can simulate long-range target probes, over-the-horizon precision strikes, and digital command platforms, which should help the PLA confront any potential opponent on an informatized battleground.[449]

The Military Regions Develop Blue Forces

The development of Blue Forces in the PLA has been steady and comprehensive. These forces are now present in all of the seven military regions of China. Not only are the Blue Forces omnipresent, they are also futuristic in nature, emphasizing informatized force scenarios instead of mechanized ones. Free play is also encouraged in place of scripted scenarios. There are literally several hundred exercises using a Blue Force that have been conducted in each military region. The following summary highlights only two or three exercises from each.

Beijing Military Region

IW exercises utilizing Red versus Blue Forces have been ongoing for several years in the Beijing Military Region. In 2000, according to a *Xinhua Domestic Service* release, an exercise deemed to be the largest electronic warfare (EW) exercise ever held in the PLA's history took place there. The exercise pitted a Red Force versus a Blue Force in a confrontation for information and electromagnetic control. It was the first time, according to the article, that the combat effectiveness of the PLA's EW equipment was tested and the first time that EW was part of combined-arms training.[450]

A 2004 article in *Renmin Ribao's* overseas edition set the stage for the unfolding of the military region's cyber activities. The article described a "laboratory of future war" located on the Inner Mongolian Plateau. Here, in what may be a Chinese equivalent of the US Army's Fort Irwin, the PLA used information technology to integrate five systems into one. These systems are: exercise direction and mobilization monitoring; battlefield simulation; assessment assistance; comprehensive support; and base management. The simulated Blue Force is composed of both traditional (armor, aviation, etc.) and

448 Wang Lin, Wang Yitao, and Wang Guibin, "A Study on the Strategy of Cultural Effects in Media Warfare," *China Military Science*, No. 6 2005, pp. 120-128.

449 Zhang, Tian, and Hao.

450 Chen Hui and Liu Yongguo, "Our Military's Electronic Warfare Capability See's New Breakthrough," *Xinhua Domestic Service*, 11 August 2000.

electronic systems.[451]

Developing a realistic Blue Force was essential to move beyond what had become "drilling and acting" during training scenarios. The inform-atized Blue Force used reconnaissance aircraft, unmanned aerial vehicles, and other systems to detect Red Force activity and conduct actual network attacks and paralysis activities. More importantly, the article states that a training simulation network allowed the base to "organize 'online' opposing force training for 'red' and 'blue' commanders and staffs." That is, there was online training in 2004, well before the 2011 announcement that it had commenced in the PLA.[452]

The *Renmin Ribao* article focused on the direction and mobilization system. The system reportedly consists of satellite position reporting and image transmission systems. It sends in real time the "geographical position and status of the actions of all key operational factors of the exercise units to a central processor and displays the information on an electronic map."[453] The system's functions include exercise control, a summation of exercise activity, the ability to intervene in activities, operational prompts, and automatic document and image generation.[454]

In September 2011 an informatized Blue Force conducted a real-troop confrontation with a Red Force. Reportedly no voice orders were given throughout the exercise. Commands can now be given online, the report noted, due to the availability of the Internet. Reconnaissance, interference, and counter measure tests have also been conducted.[455] Many announcements and descriptions of the Beijing Military Region's Blue Force exercises appear on China's CCTV, as well as in newspapers.

Shenyang Military Region

In 2005 reporters Ding Haiming and Sun Zhaoqiu wrote that the Shenyang Military Region had been utilizing a Blue Force for over a decade and that the warfare scenarios had become progressively more informatized. Computer simulations developed informatized local conflict scenarios around the globe, and this helped convert the Blue Force into a high-tech joint operation task force capable of using EW, network attack and defense, and IW means. A scripted aspect of these 2005 scenarios often allowed the Blue Force to infiltrate the command network of the Red Force. On one occasion these incursions occurred seven times during an exercise. Red Force troops were provided false instructions resulting in the erroneous dispatch of PLA troops three times.[456]

In 2007 the Blue Force utilized IW techniques to simulate operational patterns and combat methods. The military region's Red Force specialists developed tactical skills under information–oriented conditions (radio reconnaissance, electromagnetic

451 Zhang Kunping, "Laboratory of the Future Battlefield," *Renmin Ribao* (Overseas Edition), 30 January 2004, p. 6.

452 Ibid.

453 Ibid.

454 Ibid.

455 "Live News," CCTV-Xinwen, 16 September 2011.

456 Ding Haiming and Sun Zhaoqiu, "First Appearance of 'Informatized Blue Force' in the Training Field," *Jiefangjun Bao*, 11 July 2005, p. 2.

interference, and network insertion) to confront Blue Force techniques.[457] In all cases the Blue Force's success has sped up the requirement to transform the Red Force from a mechanized to an informatized force.

In 2011 Hu Jinyou, a Blue Force commander of a Shenyang regiment, stated he had just experienced his 48th Blue Force victory. The Blue Force used deception, evasion, attacks from multiple routes, and node and point destructions to cripple the Red Force's command system. The article noted that the Blue Force had studied nearly 100 combat cases to acquire lessons learned. The force had benefitted from "putting in ten years of pre-combat work for ten minutes of combat."[458] This is similar to the Chinese stratagem of "winning victory before the first battle."

Nanjing Military Region

The Nanjing Military Region, the creator of Blue Force commanders and thus Blue Force training in 1980, was highlighted by reporters in 2005 as able to simulate adversaries in future wars, thereby improving the PLA's combat effectiveness. The region established its Blue Force base in 1986, at which time it began to research future war adversaries. Key methods for enhancing this research included the 1989 Foreign Military Research Exchange Conference and the 1995 completion of a foreign military laboratory and reference room. Not long after that, a Blue *Army Tactics Teaching Materials and Research Materials for Military Region Army Operations* publication was prepared.

In 2005 Blue Force training in the Nanjing Military Region was split into two time periods. From March to the end of May the operational principles, operational characteristics, and the organization and implementation methods of a Blue Force were studied. From June to November on-site simulations were conducted. Eventually the soldiers participated in actual exercises with the Red Force. The Blue Force acquired the Red Force's frequencies, imitated the voice of the Red Force command, and successfully "moved" Red Forces. This resulted in the "utter defeat" of the Red Force.[459]

In 2008, as a result of the Blue versus Red confrontations in the region, the Red Force conducted research on eleven topics, including operational command under informatized conditions, combat firepower use, and battalion operational force assembly and coordination.[460] A 2009 report from this military region indicated that a new-type "Amphibious Blue Force" and an "Informatized Blue Force" were adding air assaults, long-range attacks, and electromagnetic jamming to their repertoire. Advanced sensor

457 Li Jingwei and Wang Shaobo, "With the Capabilities of Five-Level Confrontation and Simulation of Tens of Combat Methods of Foreign Armies—Shenyang Military Region Armored Division's 'Blue Force' Becomes Training 'Whetstone'," *Jiefangjun Bao*, 5 January 2007, p. 1.

458 Liu Jianwei and Liu Dewu, "Putting in 10 Years of Pre-Combat Work for 10 Minutes of Combat," *Jiefangjun Bao* Online, 5 November 2011, p. 5.

459 Zhao Feipend, Ni Minzhi, Peng Shimin, and Cheng Chuanjun, "Our Adversary is the PLA—Unlocking the Mystery of the PLA's First Simulated Enemy Force," *Zhongguo Qingnian Bao* Online, 23 September 2005.

460 Chen Yun and Cheng Yongliang, "Battalion's Tactical Exercise Takes to the Stage—Nanjing Military Region Group Army Explores New Ways to Adapt to Military Training Transformations," *Jiefangjun Bao*, 20 July 2008, p. 1.

technology, computer technology, mobile communication technology, and a new command automation system were being applied as well. New operational techniques included:

- Moving from confrontations based on scripts to independent and flexible confrontations
- Moving to confront tions in a systematic manner
- Moving to live force and live ammunition confrontations
- Moving to confrontations with entire divisions and regiments
- Moving to confrontations under all weather conditions
- Moving to joint operation confrontations
- Moving to confrontations of both the non combat and combat varieties
- Moving to confrontations under a complex electromagnetic environment
- Moving to confrontations that determine results instead of processes.[461]

These techniques resulted in the creation of Blue Force experts.

Blue Forces are also found in political units. In one exercise in 2011 a Blue Force sergeant was awarded a third-class merit citation for capturing audio and video from the Red Forces that he used to discover enemy plans. His award was approved quickly via an integrated command platform, where there is a path for political work that goes straight to approving officials.[462]

Guangzhou Military Region

A discussion of a trans regional movement exercise in 2009 in the Guangzhou Military Region perhaps best exemplifies how Blue Force training has progressed in the PLA. It was noted that unexpected events occurred one after the other. During the movement Red Forces were shadowed by satellites passing overhead on reconnaissance missions, and there were powerful electromagnetic jamming, harassing attacks by long-range fire, and strikes by precision weapons. In the battle area Blue Forces sent in twelve special operation subunits to harass Red Forces, and this inhibited the transport of bullets, fuel, and ammunition for some time. The organizer of the exercise said battles should be fought this way without circumstances being favorable to the Red Army. He noted that "the norm in war is predicaments, dangerous situations, and desperate straits."[463]

Further, the exercise directorate did not conduct the confrontation as a movie script, which was the tendency in the past. Soldiers were used to comparing "the exercise guidance and dispatch document to the script for a TV series." Now, only the opening situation is provided and the actions of the two sides are not constrained.[464] Refereeing

461 Dai and Ni.

462 Dong Qiang, Dai Feng, and Ou Yanghao, "Battlefield Monitoring, 'Locking in on" Your Contributions on the Battlefield," *Jiefangjun Bao* Online, 29 September 2011, p. 5.

463 Fu Wenwu, "On the Scene at a Guangzhou Military Region Motorized Infantry Division's Trans-Regional Mobility Exercise," *Jiefangjun Bao* Online, 18 November 2009, p. 6.

464 Ibid.

is now conducted using the collection of videos during the exercise, satellite locating devices, and information transmission systems, put together to "make an integrated, scientific adjudication system."[465] (This reminds one of procedures used to adjudicate controversial calls in the National Football League.) This article on the Guangzhou Military Region ended with information on a new "system," developed by an unnamed Chinese military division, that conducts automatic navigation, position locating, and short messaging without emitting any electromagnetic signals. The system supposedly can operate in all weather conditions. It "makes informatized weapons and equipment faster and more accurate," and can purportedly transmit 3,000 Chinese characters in encrypted form in 3 seconds.[466]

In 2011 the aim of the electromagnetic Blue Force was to impose a higher degree of deception on the Red Force. Chen Liwen, head of the Blue Force's electromagnetic force, stated that his goal was to set up a vivid battlefield environment for units. Red Forces confronting Chen's unit reported that the battle space felt more cunning than in the past. It now mixes truth with falsehood, as well as things virtual with things real. Once during the exercise the electromagnetic Blue Force seemed to disappear from the battlefield. This caused a commander to resume the use of wireless communications. Suddenly the Blue Force appeared and began attacking again, having used a tactic called "the empty fort strategy."[467]

Jinan Military Region

In 2007 the Jinan Military Region prepared a Blue Force that was quite unique. This army had the uniforms, weapons, operational documents, language, and habits of potential enemy groups. This unit, two journalists reported, went to the mountains in July and lived as a Blue Force for six months in every respect—language, walking, training, entertainment, food, and daily schedule. All of the officers of this group had abundant experience in information-based training.[468]

Chinese commanders of such units have ensured that Blue Forces have the proper equipment, receive proper training (to include eating with Western utensils at mealtime), utilize proper battlefield principles and tactical methods, employ creativity and innovation on the battlefield, and focus on changes made in the information-based battlefield (to include the employment of sensors, computers, mobile communication devices, assessment regulations, and so on).[469] In addition to this strict cultural indoctrination, some typical confrontational training against informatized forces is also held. For example, in 2008 the Jinan Military Region and an informatized Blue Force Command Post worked hard to create a very complicated electromagnetic

465 Ibid.

466 Ibid.

467 Xiao Zhanhong, Zhang Zhe, and Zhang Kejin, "Electromagnetic Blue Force Makes Unusual Moves Again and Again and It Is Impossible to Guard Against It," *Jiefangjun Bao* Online, 29 November 2011, p. 5.

468 Liu Yueh-shan and Chao Yi-tsun, "The Devilish 'Blue Force' Serves as a Powerful Opponent in Exercises," *Hong Kong Wen Wei Po*, 2 August 2007.

469 Ibid.

environment for the Red Force, which greatly aided the latter's training process.[470] The Red Force was made to rethink its anti-electromagnetic environment as a result.

In 2011 Blue Forces once again were successful in training against Red Forces. Deception played a key role in the Force's success (for example, computer technology was used to simulate the voice of a deputy chief director). Deception and counterdeception were reportedly practiced throughout the exercise. Red Forces snuck into Blue Force headquarters and planted a Trojan Horse virus in Blue Force computers. The Red Force perpetrators were caught, however, and no damage was done.[471]

Lanzhou Military Region

In 2007 the Lanzhou Military Region reported on the conduct of an online confrontation drill between a Blue Force and a Red Force. The Blue Force used electromagnetic jamming and surprise attacks in this particular exercise.[472] In 2008 the military region continued this focus on having the Blue Force establish a complex electromagnetic environment within which the Red Force had to operate. Other activities included Blue Force use of reconnaissance target simulation systems, remote-controlled simulation aircraft, precision fire strikes, and other characteristics of operating under informatized conditions. Most important, these confrontations were conducted under conditions of free play. The only problem to date has been maintaining a Blue Force with organizational form and spirit over time, since people are reappointed to other jobs.[473]

In 2009 journalists at a military region exercise in Lanzhou stressed that this was the "first live troop confrontation exercise in multi-arm joint information warfare."[474] The exercise included three phases: reconnaissance and counter reconnaissance, jamming and counter jamming, and destruction and counter destruction.[475]

Chengdu Military Region

In 2009 the Chengdu Military Region hosted a confrontation exercise that, like the others, emphasized the informatized command capability of both sides in accordance with guidance from the "new outline" of training. The outline stressed the preparation of the proper military mentality, military operation applications, research on operations and training under complex electromagnetic environments, research on non-war military operations, and research on security training.[476]

---

470 Li Chengjian and Zhang Shizhu, "Experts from Unidentified Group Army Help 'Blue Force' Raise Training Standards," *Jiefangjun Bao*, 21 February 2008, p. 2.

471 Zhang Nenghua, Wei Guo, and Wang Wedong, "No Restrictions Are Set on 'Blue Force' during This Drill," *Jiefangjun Bao* Online, 10 August 2011, p. 5.

472 Cui Guohui and Hou Guorong, "A Division under the Lanzhou Military Region Realizes Real Time Transmission of Target Information from the Division to Platoons," *Jiefangjun Bao*, 31 October 2007, p. 2.

473 Ma Sancheng, "Lanzhou MR Combined Tactical Training Base's Efforts to Temper 'Blue Force' for Confrontation Training Exercises," *Jiefangjun Bao* Online, 2 January 2009, p. 2.

474 "Military Report," CCTV-7, 1130 GMT, 24 October 2009.

475 Ibid.

476 He Qiang and Xu Lihua, "Everyone Can Get into Battle, Everybody Understands Command—

In 2011 a Red Force versus Blue Force exercise dubbed "Longitude-Latitude-2011" was conducted in October. The exercise practiced mapping and navigation support to campaign planning. In this case, not much was attributed to the Blue Force. Rather, the focus was on friendly capabilities. The mapping and navigation results were linked with campaign planning and preparation, operational command, and campaign actions. New geographical information systems and comprehensive battlefield situation maps were used. From these results, new ways to conduct precision command, precision strikes, and precision coordination were developed.[477]

Other Services Blue Forces

Thinking is more important than ideas…The value of a testing stone lies in providing guidance and reminders—something like what a 'lookout in the bow' will offer.[478]

The term Blue Force is not limited to the army. The Second Artillery, Navy, Air Force, and Reserve Forces all have Blue Force units, varying only in numbers, missions, and equipment. The Second Artillery has engaged in several Blue Force exercises. The Second Artillery has, like the other services, studied the composition, languages, habits, and combat documentation of different armed forces. Second Artillery Blue Force "trump cards" (operations of decisive significance) include infiltrating Red Force command and control networks and implementing electronic feints, electronic ambushes, electronic spoiling attacks, and electronic long-range strikes. Red Force weaknesses were identified as poor understanding of its enemy, inadequate information capabilities, and lax command post protection in the Jinan and Shenyang Military Regions. Creative moves by the Blue Force have motivated the Red Forces in these regions to move from mechanized warfare toward informatized warfare, which includes more use of wired relay transmissions, microwave transmissions, and wireless data transmissions, as well as high-tech camouflage equipment and false targets.[479]

According to one report, the Second Artillery Corps has used 68 battlefield directors/battlefield judges with 114 specialties. These directors/judges have been involved in 220 exercises. In a certain sense the "informatized Blue Force" that the Corps is confronting is not so much a unit as it is a future battlefield. The objective is to "pull the Red Force into future multi-dimensional warfare with system confrontation through special operations, such as network warfare and information warfare as well as stratagem confrontation in all aspects…"[480] The informatized Blue Force created

Unidentified Sichuan-Based Regiment Focuses on Improving Party Committee Members' Informatized Command Capability," *Zhanqi Bao*, 15 February 2009, p. 1.

477 Liu Xinxin and Yin Jun, "The Curtain is Lowered on the 'Longitude-Latitude-2011' Real-Soldier Campaign Exercise," *Jiefangjun Bao* Online, 30 October 2011, p. 1.

478 Ding Haiming, Wang Yongxiao, Zhang Rong, and Zhang Xianqiu, "Who is to Rival Sacred Sword—Stories of and Reflection on Second Artillery Corps Advanced Building of an 'Informatized Blue Force'," *Jiefangjun Bao* Online, 7 December 2009, p. 2.

479 *China National Defense News*, 6 June 2006.

480 Ding, Wang, Zhang, and Zhang.

electromagnetic jamming, reconnaissance and monitoring, accurate strikes, nuclear and chemical attacks, psychological strikes, special operations, and other confrontation simulations to create the proper complex battlefield environment. The directors of the Blue Force reportedly have the ability to direct and adjust confrontational means, evaluations, and evaluation standards (empirical or standard, qualitative or quantitative, etc.). The training base commander for the Blue Force uses a Sun Tzu *Art of War* quote related to his force's mission as his screen saver: "Now the general who wins a battle makes many calculations in his temple ere the battle is fought."[481]

The South Sea Fleet has also engaged in Blue Force training. During a 2009 exercise the Blue Force performed reconnaissance, deception, obstruction and jamming, and setting up 'traps' one after another. The Blue Navy forced the Red Navy Force personnel to adopt new operating procedures, none of which were specified.[482]

Reserve forces also conduct Blue-Red computerized (simulated) training. A recent exercise pitted two reserve anti aircraft artillery units against each other, which pushed confrontation training into new areas that included the construction of stratagem confrontations and holistic confrontations. The Blue Reserve Force utilized electromagnetic suppression and network attacks, as well as precision strikes, in crippling the Red Reserve Force.[483]

China's Online Blue Army Force

As noted above, the PLA had been using a Blue Force against a Red Force for several years and had discussed Blue Force tactics that used electromagnetic attacks. However, the admission in 2011 that an "online" Blue Force had been formed served as the first public admission of that unit's existence by higher headquarters. It underscores the further advancement of the PLA's cyber capabilities. Defense ministry spokesman Geng Yansheng stated that the Blue Force was not a "hacker army" and that China's intent was to develop a strong cyber defense so that it would not be at the mercy of other world powers. The "Cyber Blue Force" in the Guangzhou Military Command, the command responsible for the online unit, has 30 members, according to one report.[484] Based on the number of years that this capability has been exercised in the PLA, it is hard to believe that the command is not larger (although in this case we are only speaking of one military region).

Chinese reports on the Blue Force tend to give away its offensive character, regardless of Geng's portrayal of it as a purely defensive force. A *Renmin Ribao* report stated that "it is important for a sovereign nation to erect the best possible firewalls to deny others' attacks. And, in time of conflict, the ability to launch a counterattack to

481 Ibid.

482 Zhang Shengzhong and Zhou Yawen, "South Sea Fleet Regiment Conducts Confrontational Exercise with Live Troops with Army Unit—Powerful Lions at Sea Round Up 'Fierce Tigers on Land'," *Jiefangjun Bao* Online, 8 February 2009, p. 5.

483 Li Bin and Wang Shaoyun, "Blue Force Enters Reserve Units' Training Ground," *Jiefangjun Bao* Online, 19 November 2009, p. 6.

484 Stephen Chen, "Cyber Army is Defensive, PLA Colonel Says," *South China Morning Post* Online (in English), 27 May 2011.

disable the enemy's operations is also indispensable."[485] This report also noted that by 2020 China hopes to have trained and recruited personnel who can cope with cyber warfare capabilities.[486] The army's search for talent is diverse. Professor Jing Jiwu, the deputy director of the State Key Laboratory of Information Security, noted that offensive and defensive operations require different skills.[487] Talented recruits must be sought for both capabilities, further implying that the online army is developing offensive capabilities.

In another report, Geng Yansheng is quoted as stating that the Blue Force is a temporary program aimed at improving China's digital defenses. However, it appears doubtful that the training program is temporary.[488] Digital devices are the wave of the future and should last for a long time. Simultaneously, other analysts agree with Geng that China's cyber security is weak and very fragile. However, China is selling communication supply chain items worldwide. It is more likely they are applying the stratagem of appearing weak when strong. Meanwhile, Blue Forces continue to modernize. For example, during Vanguard 2011 it was noted that a Blue Force used electronic confrontations, cyber attacks, and aerial reconnaissance teams (unmanned drones) to conduct monitoring and interference missions against Red Forces.[489]

Conclusions

> …on the journey of developing fighting strength, it may seem that equipment is backwards but actually it is often the concept that falls behind…what cannot be delayed at all is to refresh concepts and new knowledge reserves.[490]

The construction of a Blue Force ensures that the PLA is becoming more and more familiar with Western doctrine and equipment. More importantly, the Blue Force allows the PLA to finally, after years of scripted fighting, work against a realistic OPFOR on potential future battlefields.

At the present time, while the US armed forces and elements of other nations are tied down fighting insurgents in Afghanistan, the PLA has a freer hand than other nations to focus more attention on fighting a well equipped force. The PLA's focus on the development of an expert "informatized" Blue Force presents a capable, credible advanced OPFOR for the PLA to confront, similar to what the Chinese expect to see on a future battlefield. A study of a Blue Force also tells Westerners what the PLA thinks about our strengths and weaknesses and what PLA strengths and weaknesses are as well. Reporter Stephen Chen of the *South China Morning Post* Online noted that many blue unit soldiers have been trained in hacking and defense skills. Army, air force, and navy blue units "have developed their own tactics to deal with their perceived enemies,

485 Li Hong, "China's Cyber Squad is For Defense," *Renmin Ribao* (in English), 31 May 2011.

486 Ibid.

487 Chen.

488 Liu Linlin, "PLA Creates Cyber-Defense Program," *Global Times* Online (in English), 27 May 2011.

489 CCTV-Xinwen, 4 July 2011.

490 Ding, Wang, Zhang, and Zhang.

mainland military experts say."[491]

These PLA developments are a bit surprising to China-watchers, who have witnessed countless scripted exercises over the years. In these latter events squads run behind squad leaders who brandish flags so that they can be followed, a flag that would be a dead give-away of location on a real battlefield. Mountain tops with large numbers on them were insurance that the air force wouldn't strike the wrong target. These training events may be artifacts from the past in the coming decade as the PLA introduces more and more simulations and informatized Blue Forces into their training scenarios.

The current Blue Force appears to be a worthy opponent for Red Forces, as the testimonies of Red Force commanders indicate. These commanders have now confronted a very different type of opponent on the training ground and in computer simulations. Many commanders have met defeat at the hands of the more informatized and thoughtful Blue Force. However, this experience has, in the assessment of the PLA, made Chinese commanders better. The latter now do not take anything for granted and are always on the lookout for Blue Force deception or aggression.

It would be wise for the US to closely study the development of this force over the next decade as another indicator of where the PLA is headed. Perhaps we will witness a Blue Political Force versus a Red Political Force simulation. That would be very interesting, since there is no political force in the US armed forces that equates with the PLA's. In any event, regardless of the type of potential Red versus Blue exercise confrontation, we all need to hope that the real thing never transpires.

491 Stephen Chen, "Code Blue for China's Red Army," *South China Morning Post* Online, (in English), 1 August 2011.

CHAPTER NINE: CHINA'S SYSTEM OF SYSTEM DISCUSSION: SHAPING A CLENCHED FIST

Introduction

For the past two years, several Chinese military journals and newspapers have written extensively on the topic "system of systems." In fact, it may be the most popular and specific information-related theme in recent memory. Chairman Hu Jintao noted that "it is necessary to earnestly take the effort to raise the capability for conducting information-systems-based system of systems (SoS) operations as the basic focal point for the preparation for military struggles."[492] With such top level support, it is no wonder the concept has attained wide distribution. A July 2010 posting stated that the concept is the strategic center of gravity for the present overall situation of army building.[493]

The topic of SoS was raised in the US years ago, most notably by Admiral William Owens in a 1995 article. William H. J. Manthorpe, Jr., writing in *John Hopkins Technical Digest* in 1996 about the concept, stated:

> Admiral Owens believes that C4I, ISR, and PGM systems, taken together, constitute qualitatively a quite different military potential than exists today. The interactions and synergism of those systems constitute something new and very important: a new system of systems. That system of systems is fundamentally a joint military entity. Admiral Owens is convinced that, as this broad concept emerges over the next decade, it will create a revolution in military affairs and a new appreciation of joint (that is, army, air force, navy) military operations. If the United States decides to accelerate the process by emphasizing those systems and weapons that drive the revolution, he believes that we will reach our goals years—perhaps decades—before any other nation. That will be the factor on which we base our future military superiority.[494]

Manthorpe's warning that the US may reach its goals "perhaps decades" before any other nation may have spurred Hu's desire for China to quickly study the SoS concept before falling further behind. One cannot be certain. The People's Liberation

---

492 Li Huamin, Zhang Kejin, and Fu Wenwu, "Fierce Tigers of Tashan Ask for Directions in Guangxi—Record of Actual Events about Group Army of Guangzhou Military Region Building Greater Capability for System of Systems Operations," *Jiefangjun Bao* Online, 30 July 2010.

493 Ibid.

494 Owens, W. A., "The Emerging System of Systems," *U.S. Nav. Inst. Proc.*, May 1995, pp. 36–39, as found in William H. J. Manthorpe, Jr.'s article "The Emerging Joint System of Systems: A Systems Engineering Challenge and Opportunity for APL," in *John Hopkins Technical Digest*, Volume 17, Number 3 1996, pp. 305-313. C4I is command, control, communications, computers, and intelligence; ISR is intelligence, surveillance, and reconnaissance; and PGM is precision guided munitions.

Army (PLA) has made it clear in the meantime that SoS operations are inseparable from information systems and that the concept can apply at the strategic, operational, and tactical levels of war. Of further note is that the destruction of an opponent's SoS operation is foremost in the mind of the Chinese General Staff's Third and Fourth Departments.

This chapter is divided into two parts. First, it will review the writings of Chinese journalists and experts on the system of systems concept and explain its significance and importance. The discussion represents the further development of the informationized force concept. Second, the analysis will focus on one journal, *China Military Science*, the official journal of the PLA's Academy of Military Science. The journal provided extensive coverage of the SoS concept from July 2010 to March 2011. The question that Western analysts must consider is "Are the Chinese merely playing catch up or are they instituting a different comprehensive conceptual SoS model of development that actually goes beyond the NCW concept in scope and emphasis in both its cognitive and technical parameters?" Finally, this author requests the forbearance of the reader as this chapter's material is quite dense and difficult to simplify.[495]

Web Articles

The following sub topics are short summaries of SoS articles between 2009-2011. Some author commentary is included.

The Main Principles of China's Concept: The emphasis for a system of systems concept came from above. Chairman Hu Jintao noted that such a capability was essential in order to create a formidable combat capability.[496] The leaders of the PLA recognized that they would have to follow one of two paths in the development of a system of systems concept. Leaders could build the services into a system and then merge them, or leaders could build a tri-service unified system of systems from the start. The latter path was chosen.

Some Chinese analysts believe that the SoS concept is similar to yet different from the US concept of network centric warfare (NCW). A November 2010 *Jiefangjun Bao* Online posting noted that:

> On the difference between this concept [system of systems] and the US concept of network centric warfare, Yang Lin, research fellow from a unit under a PLA General Staff Department, said that these two concepts are the same or similar in terms of the technological aspect and material basis, and that the great difference lies in capabilities and objectives because the development

495 If the material gets too difficult, a recommendation would be to proceed to section summaries or conclusions. However, the author recommends that readers not miss "A Study on Information-System-Based Network Operations Theories" on page 224. It contains important information on the PLA's digital offensive concept.

496 Luo Jun and Liu Demao, "National Defense University Holds Seminar on Theories for Building the Capability for Information System-Based System of Systems Operations," *Jiefangjun Bao* Online, 21 September 2010.

strategies and the military, economic, and technological capabilities of each country are different.[497]

NCW, according to US definitions, "focuses on the combat power that can be generated from the effective linking or networking of the warfighting enterprise. It is characterized by the ability of geographically dispersed forces (consisting of entities) to create a high level of shared battlespace awareness that can be exploited via self-synchronization and other network-centric operations to achieve a commanders' intent."[498] Network Centric Operations (NCO) is a theory which proposes that the application of information age concepts to speed communications and increase situational awareness through networking improves both the efficiency and effectiveness of military operations.[499] It appears, however, that the SoS concept is the one on which most Chinese writers focus. The PLA had earlier highlighted a concept known as "integrated network-electronic warfare (INEW)" that many thought was the equivalent to NCW. Perhaps both INEW and SoS are now in vogue in the PLA, as General Dai's description of INEW in Chapter Seven indicated.

A system is composed of concepts, rules, organization, and equipment from China's perspective. Two Chinese writers defined the SoS concept as "the union of thinking, requirements, modes, and actions. They form the basis that supports integrated joint operations."[500] Author Liu Lifeng stated that the SoS concept "propels a deep-seated reform in the armed forces organizational mode, force structure, command style, and operational thinking and style."[501] The SoS transformation is changing mechanized to informatized capabilities, fixed command posts to on-screen displays, voice commands to data relays of commands, and paper planning to quantitative computing and decision-making. Liu added that the integration of key elements and systems "should be the center of gravity."[502]

The equipment piece of the system of systems concept clearly appears in China's focus on developing high-technology reconnaissance, early-warning, sensor, and precision strike assets. Scientific decision-making mechanisms, on the other hand, appear to set some of the rules for SoS implementation. Further, there is an "information warfare cognition" element (a subjective aspect) in Chinese writings that is more innovative and creative when applied to information technologies than when considering traditional warfare models. Finally, another key to controlling the performance of the SoS lies in

497 Wang Wowen, "Learn to Use Well the Dissecting Knife of Science and Technology," *Jiefangjun Bao* Online, 18 November 2010.

498 David S. Alberts, John J. Garstka, and Frederick P. Stein, *Network Centric Warfare*, February 2000, p. 88.

499 Clay Wilson, "Network Centric Operations: Background and Oversight Issues for Congress," *CRS Report for Congress*, 15 March 2007, p. CRS-2.

500 Zhu Xiaoning and Tan Daobo, "Focus on 'System of Systems' Operations…," *Jiefangjun Bao* Online, 20 January 2011.

501 Liu Lifeng, "Clarify Basic Connotations of 'System of Systems' Operations from a Training Aspect," *Jiefangjun Bao* Online, 27 January 2010, p. 10.

502 Ibid.

control over information "flows."[503]

Tri-Service SoS. Writing for *Guangming Ribao* Online, Lin Dong from China's National Defense University stated that an invincible force on the battlefield must implement a system of systems informatization construction concept. This is because the information age has greatly reduced the effectiveness of branch-versus-branch confrontations and introduced multi-service joint confrontations. Lin believes that a tri-service unified system of systems construction is the path to take. Such a path enables an overall unified system of systems approach using information systems that enables integration (under one roof) yet distributes tasks and functions that are separate such as landing, blockade, and air-defense operations. Information superiority must be placed before everything else if this is to proceed successfully. A shift must occur from concentrating forces to concentrating efficacies. This requires open and modular units.[504]

Impact on the Military District System. A unique advantage of the military system in China is that it can quite easily (perhaps through intimidation) integrate military and civilian purposes. Author Rong Senzhi noted that "the provincial military district system is an integral part of the theater SoS operational capabilities and it is the main body to carry out national defense mobilization, therefore, the SoS operational capability building must be compatible with the core military capability building."[505] The core requirement for the PLA is that the SoS concept be capable of winning local wars under informatized conditions. To do so, the military district's SoS concept must be "an integral part of the theater system of systems operational capabilities and [it must serve as] the main body to carry out national defense mobilization."[506] Rong stated that three things are necessary to attain success: information technology must learn how to "shake hands" with operational demands; the armed forces and the civilian sectors must learn how to "hold hands;" and militia and reserve units must learn how to "join hands" with active units.[507] This shaking, holding, and joining hands help shape the SoS clenched fist. Units are implementing the SoS concept across the board. For example, the Jiangsu Military District studied Hu Jintao's thoughts on SoS operations and developed the "Jiangsu province strategic point information system" according to one report.[508]

Stratagems Remain Important. In several discussions of the system of systems concept, mention is made not only of the use of reconnaissance, control, assessment, and sensing tools but also the use of command stratagems. Stratagems enable the Chinese to attain superiority in operational constructs through the manipulation of an

503 Zhu Xiaoning and Xia Liang, "A Study of the Complex Systems Theory of Informatized Warfare," *China Military Science*, No. 4 2008, pp. 38-48.

504 Lin Dong, "How Can Our Army Become an Invincible Force," *Guangming Ribao* Online, 16 August 2010.

505 Rong Senzhi, "Thoughts on Enhancing System of Systems Operational Capability Building of Military District Systems," *Guofang*, June 2010, pp. 19-22.

506 Ibid.

507 Ibid.

508 Wu Xiuwen and Tian Yawei, "Render Troops More Capable of Conducting 'System of Systems' Operations…," *Zhongguo Guofang Bao* Online, 3 January 2011.

adversary's perceptions and actions. The utilization of stratagems requires that staffs be trained in their use and integration into a system of systems construct. Innovative methods of applying stratagems must be developed by both the civilian and military communities. Stratagems enable not only real-time support but add a dynamic aspect to support efforts. Officers are reminded to study and practice the use of stratagems in conjunction with the SoS concept during training sessions.[509] During Red Army versus Blue Army training confrontations, Red commanders are often warned to be aware of Blue commander's use of stratagems whose use is widening in information warfare scenarios. Stratagem implementation is often noted as being on a par with decision-making capability, thereby underscoring stratagems importance. A system of systems concept contains technological and cognitive aspects that, when properly considered and applied as stratagems, result in new thoughts such as new asymmetrical, deterrence, and fire strike issues.[510]

The Multiplication Effect. At a training center in the Jinan Military Region, division commander Zhou Youya stated that a system of system capability resulting in a joint combined strike force was equivalent to making 1+1>2 in a confrontation with a force without a SoS capability. It was noted that the division has a threefold jump in the number of technological personnel holding key posts in the division, reaching 600 people.[511] In addition to a joint effort, system (or structural) strength also causes a multiplication effect that increases the combat effectiveness of a nation or unit. This implies that structural attacks and not element (artillery, tanks, etc.) attacks may be the rationale behind China's focus on the system sabotage concept that often appears in the Chinese military press. Nodal attacks destroy the stability and integrity of a system thereby collapsing its utility and the utility of the elements using its assets. Chinese academicians appear to believe that SoS operations are the core operational thinking and basic operational tactic of the PLA in the information era.[512]

Total Integration is Required. As combat capabilities accumulate, the PLA feels more comfortable and confident in its abilities. PLA confidence these days borders on arrogance. Perhaps that is because they have not been as sure of their capabilities over the past two hundred years as they are today. PLA analysts often speak of integrating the system of systems concept not only within the branches of the armed forces but also with political, economic, mobilization, logistics, armament, and other operations. Stove pipes of the past will be replaced with the system of systems concept of the present. Perhaps China's military has watched the US example of using a network centric or system of systems approach and realized that it is difficult to proceed

509 Zhong Xun, "New Road Sign, New Explorations, and New Great Mass Fervors—Roundup on the Entire Army Focus on Raising 'System of Systems' Operational Capability and Pushing Forward a Transformation in Military Training," *Jiefangjun Bao* Online, 7 August 2010.

510 Song Xuewei, "Fully Use the Strength of the Populace," *Jiefangjun Bao* Online, 14 July 2010.

511 Li Guanghui and Liang Shenhu, "Basic Training Expedites Delivery Capability for System of Systems Operations," *Jiefangjun Bao* Online, 31 May 2010.

512 Huang Xing, Wang Puzhou, and Li Yun, "Rules and Circumference that Clarify the Capability for Information System-Based 'System of Systems Operations'," *Jiefangjun Bao* Online, 24 September 2010.

without implementing such a concept. Integration also encourages China's leaders to feel more prepared to win localized war under informatized conditions. The essence of the integration effort is to build an integrated command platform of three systems (automatic command, intelligence and reconnaissance, and fire assault). Three networks must be established (a field operations net, a satellite communications network, and a wireless communications network) and five superiorities established (quantity, quality, speed, decision-making, and sabotaging enemy information networks)[513] to enable success. Results of the integration process indicate the following:

> The operational system that is based on the information system takes material and energy as its foundation, takes information and decision-making as a dominating factor, and makes full use of the infiltrating, connecting, and integrating properties of contemporary information technology. The operation system is optimized through the interconnection and integration of force components and operation systems of all services and arms, and produces the effects of a system of systems. This thus brings about a qualitative leap of the armed forces' operation capability, and realizes the high-level coordination of combat actions and the high precision and high efficiency of combat results.[514]

SoS operations rely on three technologies, according to one Chinese report. These three are information technology, aeronautical technology, and long-range precision weapon technology.[515] The core concept is to in-tegrate all of these capabilities in a coherent and policy supporting method.

Officer Training. In order to implement the SoS construct the PLA, according to author Wei Wanqiang, must learn to attack and defend using the concept. Therefore officers must learn to study and design SoS operational tactics, formulate SoS tactics using advanced technologies, and incorporate precision strike thoughts when designing operations.[516] Technologies help determine the innovative and creative tactics that officers will develop. Information systems are not the only systems that should be studied. Other military systems must be studied by officers as well, such as joint operations systems, arms operations systems, and other elements that relate to military operations.[517]

Reducing the Fog of War. The SoS concept helps reduce the fog of war by integrating

513 An Weiping, "Take Information Confrontation Capability as 'Foundation Stone'," *Zhongguo Guofang Bao* Online, 30 December 2010.

514 Pan Shouyong, "Scrutinize the Subjective Change of the War Pattern—on the Content and Significance of System Operations Based on the Information System," *Jiefangjun Bao* Online, 15 April 2010.

515 Fu Helin and Lin Mingxian, "Three Major Technologies Underpin Armed Forces' Capability of Conducting 'System of Systems' Operations," *Zhongguo Guofang Bao* Online, 16 September 2010.

516 Wei Wanqiang, "Attach Importance to 'Tactical Operations' Involved in 'System of Systems' Operations," *Zhongguo Guofang Bao* Online, 24 February 2011.

517 Zhang Ming and Chen Yingjian, "We Should Stop Eying Information Systems Only," *Zhongguo Guofang Bao* Online, 14 October 2010.

efforts and it reduces the bottleneck for joint operations. An informatized system of systems operation produces an overall unified information-dominant integrated system that allows for the distribution of tasks and functions that are separate, such as landing, blockade, and air-defense operations. This requires leaders to shift from concentrating forces to concentrating efficacies. For example, it is now possible to construct an all-army unified public network into which "all information systems and informatized armaments are loaded, which simplifies the numerous interfaces into a single network access interface."[518] Another method for piercing through the fog of war is through the use of military requirements on the "Internet of Things."[519] As one article noted

> The focus of the core of military requirements on the Internet of Things is on systematically achieving effective operations in all directions, in the entire temporal domain, and in the entire spectrum by centering on battlefield situation perception, intelligence analysis and assessment, operational process control, and other factors so as to pierce through the "fog of war," increase the transparency of friendly forces on battlefields, and comprehensively raise the capability for information-based SoS operations.[520]

The article noted that the main military application of the Internet of Things (listed as one of the five major emerging strategic industries of the state) is to coordinate systems and elements such as battlefield perception, intelligent control, and precision operations; to build an all-dimension early warning system to make up for other equipment shortcomings; and to use nanobiosensors as a weapon network monitoring system, among other issues.[521]

Lin Dong, mentioned earlier, advocated the implementation of an all-army unified public network into which all information "systems and informatized armaments are loaded." The network would simplify interfaces and connect everyone via a network intermediary, thereby providing a partial solution to the fog of war.[522] In this regard the Chinese are interested in involving civilian technologies in their system of system capability infrastructure in a comprehensive manner. Civilian support should be synchronized and dynamic such that armament battlefield system support (logistics, command and control, etc.) is enhanced.

---

518 Lin Dong, "How Can Our Army Become an Invincible Force," *Guangming Ribao* Online, 16 August 2010.

519 The definition of "Internet of Things" can be found on *Wikipedia*. There it states that in computing, the Internet of Things "refers to the networked interconnection of everyday objects." However, it also notes that the definition may require cleanup to meet *Wikipedia's* quality standards. Another source notes that "from *anytime*, *any place* connectivity for *anyone*, we will now have connectivity for *anything.* Connections will multiply and create an entirely new dynamic network of networks—an Internet of Things." See http://www.itu.int/osg/spu/publications/Internetofthings summary.pdf.

520 Unattributed article, "Internet of Things: Making Big Steps Toward Battlefields," *Jiefangjun Bao* Online, 9 December 2010.

521 Ibid.

522 Lin Dong, "How Can Our Army Become an Invincible Force," *Guangming Ribao* Online, 16 August 2010, at http://www.gmw.cn.

Subelements are Important. A system, of course, is composed of one or several subcomponents. Key sub elements include reconnaissance, command and control, early warning, strike, and support elements, (among others) according to Chinese authors.[523] In this sense the Chinese seem to echo Admiral Owens C4I, ISR, and PGM system integration concept. However, for some Chinese theorists, some elements (such as the support element) include items that are not focal points in the US system. For example, the "three warfare" capabilities (psychological, law, and public affairs operations) are one support item that the West does not recognize as consistently as an element of its NCW concept as the Chinese do with their SoS concept. Further, according to an article found at *Jiefangjun Bao* Online, "The operational system has a multitude of sub-systems and has a multi-tiered structural framework. The sub-systems have close and complicated relations, and are related to social, political, military, economic, technological, and environmental factors."[524]

A New Quality Fighting Force. Journalist Lu Junjie writes that the system of systems operational capability based on information systems is a "new-quality fighting capacity" that combines sensing, real-time command and control, precision strike, all-dimension protection, and focused support into a comprehensive whole. It will be a basic form of fighting under informatized conditions.[525] On the one hand, some characteristics remain the same such as the use of "levels" similar to the levels of war. A system of systems configuration of forces still involves attacks in the information and electromagnetic domains on the first level, and it still has a hierarchical nature in the method of attack. For example, US aerial attacks usually involve early warning and command aircraft, then electronic jamming aircraft, and only then F-14 and F-18 fighters.[526] On the other hand, the key to winning the strategic initiative in local wars under informationized conditions requires integrated joint forces according to many PLA authors. These forces must be able to attack an adversary's key nodes and critical targets from an initial defensive posture. The more "asymmetrical" the attack, some think, the better the chances for success.

Differences in the Two Systems. The US military requires systems that work now in support of their many ongoing operations. The PLA, however, seems to be putting more thought into innovating than into actually building a system of systems capability perhaps because they have more time to do so. China is not involved in three conflicts nor have they been for the past several decades. This may be one of the big differences between China and the US. The Chinese are less pressed and have more of an opportunity to reflect and critique other nation's approaches to these issues and then analyze and innovate their own approaches. In fact, China's official news

523 See, for example, Guan Lifeng, "Improving the Powerful Engine of System Operations Capabilities: Thoroughly Reviewing the Information Systems in Operational Systems," *Jiefangjun Bao* Online, 4 February 2010.

524 Pan Shouyong.

525 Lu Junjie, "Elementary Introduction of 'New-Quality Fighting Capacity'," *Jiefangjun Bao* Online, 27 May 2010.

526 Ahao Hui and Han Dongyan, "We Should Also Attach Importance to the Use of Military Forces According to the Arrangement of Levels," *Jiefangjun Bao* Online, 14 July 2010.

service for overseas Chinese (*Zhongguo Xinwen She*) noted in 2010 that a pilot project for command confrontation under informatized conditions is underway in relevant PLA regions. The General Staff noted that raising system of system confrontation capabilities will continue to be researched and implemented over a period of three years.[527] Such capabilities are the basic feature of information-era wars that highlight comprehensive integration as a basic method of system of systems construction.[528] Only the SoS construct can offer China hope to integrate strategic, campaign, and tactical intelligence and reconnaissance.

Operational Theories and SoS. One report from the Jinan Military Region noted that fifty new battle operational methods of system of systems offense and defense have been constructed. The report added that the issues of integration, synchronization, real-time sharing, and the development of distributed command and control assets demonstrate the power of the SoS operational theory.[529] Other theories or methods were explored as well. One of interest was the method of meta-synthesis, used in the research and innovation of operational theories. It is an SoS approach in which wars are viewed from the national and international perspectives and contemporary wars are viewed from a historical perspective. Meta-synthesis stresses qualitative-quantitative synthesis. The value of data is evaluated from a qualitative perspective and the appropriateness of the experience is verified from a quantitative perspective. This puts operational theories under repeated qualitative and quantitative research and verification. Vertically, historical issues, practical issues, and future potentialities are combined together; horizontally, things inside the PLA, inside China, and in the world are organically linked together, along with material and spiritual things, tactical and technical things, and everything else that is related, thus comprehensively leading to the emergence of an all-inclusive operational theory.[530]

Problems Implementing the SoS Concept. Several problems were highlighted during the course of the SoS discussion. Some of those issues were:

- Imperfect communication facilities, stand-alone systems, and poor practices exist in some PLA information systems which restrict the PLA's SoS capability[531]
- "Three too-many and three too-few" is the PLA's way of stating that there are too many organized combat forces, conventional forces, and single-purpose specialty forces and too few organized rescue and relief forces,

527 Liu Feng'an and Tao Shelan, *Zhongguo Xinwen She*, 0246 BMT, 15 March 2010.

528 Zhang Zhaoyin, "Guide the Transformation of the Armed Forces with the Building of System of Systems Operations Capabilities," *Jiefangjun Bao* Online, 18 March 2010.

529 Wei Bing, "Whole-System Training Strengthens All Battle Posts: The Communications Units of the Jinan Military Region Actively Explore Ways of Element Integration Training," *Jiefangjun Bao* Online, 31 October 2010.

530 Liu Jixian, "We Must Strengthen Research on and Innovation in Operational Theories," *China Military Science*, No. 2 2010, pp. 1-14.

531 Yuan Jiusheng and Wang Zhangping, "Looking at Building of 'System of Systems' Capability through 'Tenting Effect'," *Jiefangjun Bao Online*, 16 December 2010, p. 10.

forces with unique specialties, and comprehensive support forces[532]

- A problem remains in overstating successes at the expense of problems in training. More self-criticism is called for in SoS operations, which are difficult to conduct and should expose numerous problem areas to fix now in peacetime
- China's SoS concept requires the mastery of complexities, without which one is sunk into an inescapable chaotic quagmire.[533]

China Military Science Articles

During 2010, PLA analysts wrote extensively on the SoS concept. The concept appears to be the basic form through which combat capabilities under informationized conditions are expressed and future war plans formulated. It is also, according to several Chinese sources, a method through which to review and adjust China's national defense mobilization system.

The rationale behind the development of this concept is that the Chinese believe future wars will not be one-on-one confrontations as in the past; rather they will be confrontations between systems that have now become the basis of combat power and the strategic option most likely to guarantee success for the PLA. SoS operations are also deemed to be the core of the transformation of the method for generating combat capabilities.

If there was a focal point for the SoS topical discussion in 2010 it was the journal of the Academy of Military Science, *China Military Science*. The journal dedicated two special sections of Issues 4 and 5 to "Information-System-Based System of Systems Operations" of various types (maritime, nuclear, political, logistical, etc.). Casting the net of SoS topics so wide appears intended to ensure that China, in case of conflict, is prepared to promptly mobilize its forces and resources across the board. They envision the SoS concept as a primary key to future success on the battlefield.

The "theme forum" section of those issues of *China Military Science* highlighted the following topics:

Issue 4, 2010 Theme Forum: Theoretical Research on Systems Operations Based on Information Systems

1. "Preliminary Understanding of Information-System-Based System of Systems Operation Capabilities"
2. "A Study of the Mechanism of Information-System-Based System of Systems Operations"
3. "On the Composition and Basic Mode of Generating Information-System-Based System of Systems Operational Capabilities"
4. "Considerations for the Guidance of Information-System-Based System of Systems Operations"

532 Rong Senzhi.

533 Meng Zhaobin, "Mastering Complexities: Path to Subduing Enemies in Future Battlefields," *Jiefangjun Bao* Online, 17 November 2011, p 10.

Issue 5, 2010 Theme Forum: Theoretical Research on Systems Operations Based on Information Systems

1. "Build a New Type of Operational Force Capability System Based on Information Systems"
2. "A Study of Information-System-Based Network Operations Theories"
3. "Thoughts on Raising Information-System-Based Maritime System of Systems Operations Capability"
4. "Information-System-Based System of Systems Operations Command Capability and a Study of its Applications"
5. "Information-System-Based System of Systems Operations Adapt to the Requirements of Systems Operations Based on Information Systems and Promote the Reform and Innovation in Army Political Work"
6. "A Study on Improving Core Logistical Support Capability in Information-System-Based System of Systems Operations"
7. "On Training Modes of Information-System-Based System of Systems Operations Capability"
8. "A Study of the Application of Nuclear, Biological, and Chemical Defense Forces Based on Information Systems"

Of the twelve articles highlighted above and discussed below, representatives of the Naval Command Institute, the Academic Research Department of the General Logistics Department, National Defense University, Nanjing Army Command Academy, the Academy of Military Science Research Center of Military Political Work, and the Chemical Defense Command Engineering Academy wrote one article each; representatives from the Academy of Military Science wrote two articles; and representatives of the Shijiazhunag Army Command Academy wrote five articles (on training, force capability, command capability, the SoS mechanism, and the composition of a SoS operation). The following discussion will highlight the salient issues addressed in each of these articles.

Issue Number 4 2010

Preliminary Understanding of Information-System-Based System of Systems Operation Capabilities

Major General Ren Liansheng of the Academy of Military Science opened the discussion on SoS operations. He stressed that the basic form of combat capabilities under informatized conditions is the information-system-based SoS operation capabilities, capabilities that will enable the PLA to win local wars under informationized conditions. The SoS concept provides strategic guidance for the PLA's informatization-building effort. His discussion set the stage for others to follow in the pages of *China Military Science*. Ren noted that Chinese Chairman Hu Jintao first discussed such

capabilities in 2005,[534] indicating that the idea has been under consideration for some time.

"Information-system-based SoS operation capabilities" refers to the systemized operational capabilities that generate an amplifying effect through the integration of real-time sensing, effective command and control, precision strike, rapid maneuvers, all-dimensional defense, comprehensive support, and other operational capabilities. The sharing of information results in structural optimization and system synthesis, producing a qualitative leap in operational capabilities, coordination, precision, and efficiency. The coordination and concentration of information power results in strikes against decisive targets in decisive locations at decisive times. This increases the effectiveness of firepower strikes exponentially.[535]

The new technological era is demanding on military personnel. Commanders are required to have scientific and cultural knowledge, to be able to exercise command and control in modern war, and to be able to use new means of command. The information technology era also promotes innovation in military theories.[536] Ren adds that

> War is no longer a contest among the various operational units but rather a system vs. system contest based on the comprehensive integration of various combat platforms and various combat elements. The struggle for information control goes on throughout the course of operations and infiltrates into every aspect of war. Information supremacy becomes the key to seizing air supremacy, sea supremacy, and supremacy over other operational domains.[537]

Ren concludes that in the building of a SoS operational capability the growth point must shift from traditional fields of operations to new fields more pertinent to the expansion of national interests.[538] This may indicate a less than subtle shift in PLA strategies worldwide. Ren further emphasizes that China should adopt a concept of asymmetrical development (taking local characteristics and operational needs into consideration) and should promote military-civilian integration (abandoning the idea of working behind closed doors) so that a new type of armed forces can be created, one capable of fighting and winning local wars under informatized conditions.[539]

A Study of the Mechanism of Information-System-Based System of Systems Operations

Ping Zhiwei, a deputy director of the Campaign and Tactics Department of the

534 Ren Liansheng, "Preliminary Understanding of Information-System-Based System of Systems Operational Capabilities," *China Military Science*, No. 4 2010, pp. 26-33.

535 Ibid. Military information systems refer to those systems used in combat operations, primarily command and weapon systems. The term "system-based" refers to integrating elements, supporting joint systems, and optimizing structural capabilities.

536 Ibid.

537 Ibid.

538 Ibid.

539 Ibid.

Shijiazhuang Army Command Academy, and Majors Zeng Xiaoxiao and Zhang Xuehui, both from the Combined Tactics Teaching and Research Office of the same department and academy, discussed operational mechanisms of the SoS concept. They listed five aspects of the concept, namely domain control, system sabotage, effect control, integrated joint action, and self-organized collaboration.[540]

With regard to the domain control mechanism, the authors note that control of any single domain does not guarantee the seizure and maintenance of the battlefield initiative. Comprehensive (air, sea, space, electromagnetic, etc.) domain control is required. Information control remains a most important topic, however, in that it helps determine the outcome of operations.[541]

The system sabotage mechanism aims to damage the structure of an adversary's operational system, or at least disrupt it. The system to system confrontation and sabotage concept offer the capability to paralyze an adversarial operational system. Confrontations are aimed at severing an opponent's campaign and tactical systems. Sabotage is aided through maneuver and precision strike capabilities that keep an adversary guessing as to the place and time of a final assault.[542]

The effects control mechanism implies the ability to precisely control the operational process in order to achieve a desired result or to impose anticipated effects on an adversarial force. A real-time assessment of these effects is the key to controlling operations (via reconnaissance, intelligence, etc.). Based on such assessments, commanders can now make ad hoc adjustments to provide strikes at critical times and places.[543]

The integrated joint action mechanism refers to "winning operational victories by means of joint actions in multi-dimensional operational domains with information support" as various component elements of SoS operations seamlessly connect network-based information systems for high-level integration and for assisting decision-making. This allows for coordinated responses to various scenarios. The systems that the authors named were the intelligence, reconnaissance, command and control, fire strike, three-dimensional maneuver, and information countermeasure systems. The "adhesive agent" for turning these systems into integrated and networked commodities is information. Near real-time assessments allow for the integration of "perception-judgment-decision making-strike" assessments at all command levels.[544]

Finally, the self-organized collaboration mechanism is a SoS operational mechanism defined as the ability to enable forces to adjust one's actions to battlefield changes according to certain rules of collaboration, based on sharing battlefield information while receiving no input from higher headquarters. That is, some subsystems of larger systems act with initiative and creativity to carry out a plan. The subsystems either adjust

---

540 Ping Zhiwei, Zeng Xiaoxiao, and Zhang Xuehui, "A Study of the Mechanism of Information-System-Based System of Systems Operations," *China Military Science*, No. 4 2010, pp. 34-43.

541 Ibid.

542 Ibid.

543 Ibid.

544 Ibid.

collaboration plans or establish a new relationship if collaboration is interrupted.[545]

On the Composition and Basic Mode of Generating Information-System-Based System of Systems Operational Capabilities

Lieutenant Colonel Yan Zhensheng, Major Liu Haijing, and Major Feng Wei, also from the Shijiazhuang Army Command Institute, further stressed that the SoS operation is the main form of joint operations under informatized conditions. The authors note that SoS operations create a multiplication effect generated via the integration of various systems. No longer is warfare based on physical destruction between individual weapon platforms but rather on a confrontation among SoS as a whole. Here the release of combat effectiveness will take place as a whole and not as individual elements.[546]

Information has become the objective criteria through which to analyze SoS operational capabilities. The flow path for information in an information system, the authors note, is via acquisition (reconnaissance), processing (consolidation, analysis, sharing), and utilization (directing material and energy flows). The processing phase is usually the most important since it ascertains whether the information acquired is relevant or not. Subsystems impact one another only when they interact and there is a function coupling relationship.[547]

Yan, Liu, and Feng conclude that the goal of a comprehensive integration effort is to "link up the internal parts of the operational system horizontally and vertically and link up the command systems seamlessly, achieve multi-service, multi-level, and multi-element joint action as a whole."[548] This will allow for an "overall surge of SoS capabilities" at the tactical, campaign, and strategic levels. A recommendation was to build an operational data center, an intelligence and situation center, and other centers that are secure and disaster proof.[549]

Considerations for the Guidance of Information-System-Based System of Systems Operations

SoS operations enable both sides in a conflict to advance along technical, advanced, and comprehensive lines of strategic thought. Author Senior Colonel Luo Xiangde from the Nanjing Army Command Academy notes that strategic SoS thought for China is "a strategic thinking activity in which subjective ideas are manifested through objective realities."[550] The article expresses objective realities in terms of information systems and subsystems while subjective ideas are expressed in terms of innovations and psychological activities.

---

545 Ibid.

546 Yan Zhensheng, Liu Haijing, and Feng Wei, "On the Composition and Basic Mode of Generating Information-Based-System of Systems Operational Capabilities," *China Military Science*, No. 4 2010, pp. 44-50.

547 Ibid.

548 Ibid.

549 Ibid.

550 Luo Xiangde, "Considerations for the Guidance of Information-System-Based System of Systems Operations," *China Military Science*, No. 4 2010, pp. 51-58.

An information system includes command and control, intelligence, reconnaissance, communications, early-warning and detection, security, information confrontation, and other subsystems. An information system advantage can generate both decision-making and action advantages. The technical foundation, system construction, and overall effectiveness of SoS objective operations also take into consideration the political, economic, military, diplomatic, and other issues involved in future SoS operations.[551] The comprehensive nature of the integrated SoS approach indicates that "The strategic guidance for information-system-based system of systems operations not only cannot completely rely on information warfare's networked attacks but also cannot rely on the cumulative destruction of individual targets to defeat the other side, as was the case in mechanized wars."[552] Perhaps for this reason subjective factors have become very important.

The use of objective factors can "overturn the system balance of the system of systems operations technically to obtain combat opportunities."[553] This appears to be China's strategic goal, to upset the balance of internal systems and combat elements, which thereby upset the technical balance in an adversary's operational system. To stop the flow of information and upset balance, one can (1) destroy the interaction and exchange among information, material, and energy flows within the operational system or (2) overturn the system's internal and external balance and paralyze the whole or parts of the system. One can reach the goal of controlling the enemy by making the enemy lose control of itself.

The comprehensive use of various means is required to thwart an adversarial force. Studying information-system-based SoS operations helps guide informatized war, as well as preparations for implementing inform-atized war. There remains a gap between establishing strategic guidance for the conduct of SoS operations and their implementation in order to win informatized war.[554]

Interestingly, Luo's discussion of SoS operations also included a brief description of a Chinese concept known as integrated network-electronic warfare (INEW), a concept that appeared nearly ten years ago. According to this concept computer network warfare disrupts the processing and use of information while electronic warfare disrupts acquiring and forwarding information. Information systems include four links: information acquisition, transmission, processing, and utilization. Information acquisition and transmission rely on electromagnetic frequencies, while information processing mainly relies on computer networks. Information utilization relies on informatized weapons platforms. The targets of electronic attacks are then information acquisition, transmission, and utilization links while the targets of network attacks are information processing systems. INEW attacks increase the probability of paralyzing an entire information system.[555]

551 Ibid.
552 Ibid.
553 Ibid.
554 Ibid.
555 Ibid.

There was a cognitive factor interlaced in the SoS discussion. The article stated that modern means of media are part of SoS operations. Public opinion propaganda and psychological warfare attacks are used to guide the public's psychological inclinations. To thwart an adversary's threat, the use of psychological, public opinion, and legal struggles must be carried out through information resources. The creation of a unified approach both within and outside the country is necessary while simultaneously undermining the enemy's will and conviction, whether it be decision-makers or just the general populace. This requires a combination of military and non-military actions.[556]

Finally, the article argued that anti-psychological training is required in the PLA force. A balance must be maintained among a soldier's cognition, sentiment, and will. Team spirit serves as a multiplier of SoS operations. Commanding officers are a particular focal point for anti-psychological training, as they represent the heart of the armed forces.[557]

Issue 4 Summary

A variety of institutes appear to be studying the SoS operational construct. The Nanjing Army Command Academy, the Shijiazhuang Army Command Academy, and China's National Defense Academy all contributed to the discussion in Issue 4 of *China Military Science*. The SoS operational concept was viewed as a basic form of combat capabilities, one used in combat operations and especially in command and weapon systems. When integrated, SoS capabilities offer a multiplication effect in both a technical and cognitive sense. The SoS operation was also described as a mechanism designed to enable control over events. Finally, the SoS thought process was linked with the concept of strategy. Author Luo Xiangde noted that it is an "activity in which subjective ideas are manifested through objective realities,"[558] which is exactly how some Chinese military authors define strategy. Also of particular interest was Ren Liansheng's comment that when building the SoS operational capability, the growth point should be in fields "more pertinent to the expansion of national interests."[559]

Issue Number 5, 2010

Build a New Type of Operational Force Capability System Based on an Information System

Authors Colonel Zhang Hong and Captain Yu Zhao of the Shijiazhuang Army Command Academy write that "networking early-warning and detection equipment may break the separate institutional structure of the intelligence and reconnaissance systems in various services and arms, change the condition of their isolated operations and duplicated reconnaissance, and facilitate the complementarities of their efficacies in terms of time, space, and frequency domains."[560] That is, it is hoped that the SoS

556 Ibid.
557 Ibid.
558 Luo.
559 Ren.
560 Zhang Hong and Yu Zhao, "Build a New Type of Operational Force Capability System Based

operation will overcome the obstacles posed by separate structures. An important observation the authors make is that informatized battlefield demands will give rise to new combat forces, to include information operational forces (electronic countermeasure and network warfare units), space military forces (who will occupy the absolute commanding heights on informatized battlefields), and an unmanned operational force (which will move from a supporting to an operational role).[561]

Zhang and Yu note that "SoS operations require the integration of battlefield perception, information transmission, command and control, information offense and defense, network countermeasures, and precision strikes with the information system as the bond."[562] The foundation for a battlefield perception concept is sharing intelligence information. The data link in such an operational system includes a command guidance network, an operation cooperation network, a weapons control network, and a battlefield situation information distribution network. An information standardization system must be developed as well.[563]

For weapon systems it is necessary to install friend or foe identification systems, navigation and positioning systems, and broadband high-speed data links to missiles, artillery, aircraft, and other fire strike weapons. It is necessary to construct the command, control, communications, computer, kill, intelligence, surveillance, and reconnaissance (C4KISR) capability and to effect the integration of information warfare and firepower strike means. Engagements with adversaries will occur in tangible domains (ground, sea, air, space, and electronics) and in the intangible domains (the cognitive and psychological). These domains will offer more battle-fighting patterns and combat methods than those previously occurring. SoS actions are manifested mainly as time and space collaboration and synchronization.

A Study on Information-System-Based Network Operations Theories

PLA Senior Colonels Li Daguang and Han Yufeng of China's National Defense University wrote on networks and furthered the discussion on SoS. They stated that the guiding principle of information-system-based network operations is active network defense. However, defense is not the only activity of network operations. The authors stress that the theory has offensive and defensive aspects and these are integrated into network operations, representing a major difference from traditional operations. This is because dominance in cyberspace determines who gains the strategic initiative in twenty-first century warfare. First, network technology determines network tactics (network reconnaissance software, attack software to include paralysis, obstruction, and deception software; network software allows for online intrusion, long-distance theft, manipulation, control, and attack confrontations). Technology can also determine operational methods. Second, network attack operations are easier to conduct than defensive operations, encouraging an offense-to-defense cost effectiveness or advantage

on an Information System," *China Military Science*, No. 5 2010, pp. 10-16.

561 Ibid.

562 Ibid.

563 Ibid.

ratio of 1:100. Invisibility encourages offensive penetration. Third, warfare is socialized, meaning that there is closer military and civilian interconnection and exchange of technology than ever before.[564]

The total strength of a nation to conduct network operations hinges on its information infrastructure. The latter includes the resources, databases, transmission networks, application systems, and soft and hard operational platforms that can be employed. When the appropriate infrastructure is present, then a side can take advantage of means and methods to control, disrupt, and destroy the systems of an opponent. The authors note that "the emphasis is on launching offense as defense and integrating offense and defense under the network's overall defensive posture, using active offensive operations to achieve a defensive goal."[565] The offense is stressed since it is easier and has higher maneuverability than defense. When subject to an attack, the main force has to have an effective offensive counterattack force available for deployment. To help prevent attacks, intrusion methods must be studied during peacetime to prevent their employment against friendly systems, while at the same time hiding them in enemy systems.[566]

Thoughts on Raising Information-System-Based Maritime System of Systems Operations Capability

Senior Captain Jiang Lei, a professor at the Naval Command Institute, wrote that specific capabilities are required today, including maritime information gathering, transmission, processing, countermeasure development, and support. Peacetime-wartime integration is also a must, since the use of maritime military forces in non-war capacities is growing as more and more sea-crisis events arise.[567]

The maritime force must change from a navy-based force to a three-services force, one that creates an all-service, all-arms joint maritime operational force. A forest of "chimneys" must be replaced by one big integrated system capable of fighting along coastal waters or in the open sea. Maritime operational space is now characterized by greater depth and thus requires greater integration of assets and the extended use of space information support assets. The key to success, as in other areas, is attaining electromagnetic control, followed by air and sea control. A comprehensive SoS operation consists of reconnaissance and survey, information processing, firepower strikes, battlefield maneuvering, offensive and defensive actions, command and control, and assistance and support.[568]

China must create a national defense communication system that uses hubs and fixed locations as support, uses optical cable as the primary means of communication, and supplements these means with others. A mobile communication system that uses

564 Li Daguang and Han Yufeng, "A Study on Information-System-Based Network Operations Theories," *China Military Science*, No. 5 2010, pp. 17-23.

565 Ibid.

566 Ibid.

567 Jiang Lei, "Thoughts on Raising Information-System-Based Maritime System of Systems Operations Capability," *China Military Science*, No. 5 2010, pp. 24-31.

568 Ibid.

short wave, ultra-short wave, and microwave relays should also be created, along with a space-based communication system that uses strategic communication satellites and tactical communication satellites as platforms to transmit intelligence, support, and command information about the entire maritime battlefield.[569]

The SoS operation uses information to determine the release of battlefield energy at the proper time and place and to direct material flows to proper locations. A maritime SoS operational capability should

> Make skillful use of the multi-frequency, multi-level, multi-dimensional sea, land, air, and space-based information system and, through the use of space reconnaissance satellites, early warning satellites, airborne early warning vehicles, large comprehensive electronic reconnaissance ships, and pilotless reconnaissance planes, enable the various types of intelligence and reconnaissance equipment, as well as the various levels of intelligence reconnaissance equipment systems, of the participating forces to conduct all-hour, all-weather scouting and monitoring of the maritime battlefield and collect intelligence and information.[570]

Jiang did not ignore the cognitive aspect of maritime operations either. He wrote that network-telecommunications integrated information warfare, public opinion warfare, and psychological warfare have now become important forms of operations.[571]

Information-System-Based System of Systems Operations Command Capability and Study of its Applications

SoS command capability refers to the capability of commanders and command organs to plan, coordinate, and control operational actions of forces of multiple services and arms that are supported by information systems. The concept is designed to deliver precise strikes on targets and sabotage key system nodes.

Senior Colonels Li Yanbin and Zhang Ce and Major Wu Hongqi, who work at the Shijiazhunag Army Command Academy, write that the concept of SoS is the hub where other capabilities converge. Integration is thus the primary factor determining SoS capability. It affects the performance and capabilities of all other components (battlefield sensing, precision strike, long-range power projection, information offense and defense, all-dimensional protection, and comprehensive support). The recent wars in Iraq offer further proof that the ability to attack an adversary's command capability while protecting one's own is the most important component that can lead to victory. It is the "nerve center for the precise release of efficacy in SoS operations."[572]

The command capability's structural optimization and modular integration are its

569 Ibid.

570 Ibid.

571 Ibid.

572 Li Yanbin, Zhang Ce, and Wu Hongqi, "Information-System-Based System of Systems Operations Command Capability and the Study of Its Application," *China Military Science*, No. 5 2010, pp. 32-41.

greatest characteristics. Combined and synchronized planning and decision-making capability refers to a commander's ability to make interactive plans from different places and make synchronized joint decisions through comprehensive electronic information systems. This allows the commander and his command organs to control not only an operation's tempo but also its initiative. This is the pivotal element of the SoS operation's command capability.[573]

PLA planning and decision-making pre-practice activities are influenced by the "making judgments beforehand—formulating contingency programs—conducting operational experiments—making revisions and improvements—enforcing impromptu application" paradigm.[574] The PLA establishes an advanced operational experiment and simulation system to respond in an interactive way for the synchronized discharge of command efficacy. This is one way that the effect of the system can be greater than the sum of its components' functional efficacy. Another way is the development of superior stratagems. Command confrontation capability in typical actions refers to stratagem thinking to offset an adversary's stratagems. Commanders must be able to carry out command stratagem confrontation while protecting one's own side from attacks from an adversary's system.[575]

The SoS operational command relies on a mega-system that is interconnected and able to communicate with all sub-systems. Network-based command organs act as hubs. Supporting these "node-style" command organizations are the real-time sharing of battlefield postures and the all-area distribution of command information systems. Command organs must be distributed to different locations to ensure their survivability. Reliance on these systems enables commanders to depart from traditional decision-making based on subjective experiences to decision-making based on the information-driven multi-dimensional integrated reconnaissance and detection systems. Information superiority is thereby turned into battlefield dominance decisions made synchronously and interactively. Networked command and control platforms also allow relevant political, economic, diplomatic, security, scientific, and technological fields to be gathered together.[576]

A precondition for commanding SoS operations is the accurate determination of the positions of both friendly and adversary sides to a conflict. Precise control of targets is also required for effective command and control, making battlefield control the crucial link in the use and implementation of operational command capability. This capability and that of operational optimization can be exercised in simulation laboratories.[577] The authors write that

> Operational simulation in essence provides an 'operation lab' in which the operational environment can be simulated, stratagems and plans can be tested,

573 Ibid.
574 Ibid.
575 Ibid.
576 Ibid.
577 Ibid.

> their defects can be found and examined, the results of such stratagems and plans can be predicted, the efficacy of the weapon systems can be evaluated, and new operational ideas can be developed.[578]

Information-System-Based System of Systems Operations Adapt to the Requirements of Systems Operations Based on Information Systems and Promote the Reform and Innovation in Army Political Work

This article, authored by Wu Zhizhong, Wang Zhengdong, and Huo Qicheng, stated that in SoS operations a "lifeline" must be extended to participants, albeit a political one. SoS operations can be viewed as a political trial of strength as one force confronts another that may be more powerful. It is necessary, the article states, to rely on the PLA's political, human, and spiritual superiority to overcome disadvantages in the size and strength of an opposing force and maintain an adequate political counterbalance. An SoS operation should not be viewed as only a hard kill asset; it can also serve as a soft kill asset that can overcome all obstacles if properly studied and applied.[579]

SoS operations are composed of four elements: systems, theory, laws and regulations, and personnel. SoS training is needed for command, administrative, specialized, and operational personnel in all areas, to include political issues. The focus must be on developing the proper skills to excel at SoS operations in each area. PLA forces must learn from foreign forces the ins and outs of SoS operations. Proper incentives must be provided to interest personnel in this field of study, from monetary incentives to those of a business nature. Political work networks and service systems have made a qualitative leap in capabilities over the past few years, which improve PLA chances for success in the political field.[580] A final recommendation was to do the following:

> We must do our utmost to actively create conditions for political cadres, making arrangements for more wartime political work exercises in the context of information SoS operations, making arrangements for large online exercises and, during exercises, examine and improve the political work systems and mechanisms in systems operations, tempering personnel, training, and improving political cadres' skills in systems operations.[581]

A Study on Improving Core Logistical Support Capability in Information-System-Based System of Systems Operations

Senior Colonels Gao Dongguang and Wang Youlin of the Academic Research Department of the General Logistics Department wrote on the importance of logistics in an era defined by SoS operations. The content of such operations must include a high-degree of information integration; precise and focused support; the ability to integrate

578 Ibid.

579 Wu Zhizhong, Wang Zhengdong, and Huo Qicheng, "Adapting to the Requirements of Information Systems-Based System of Systems Operations to Promote Reform and Innovation in Military Political Work," *China Military Science*, No. 5 2010, pp. 42-46.

580 Ibid.

581 Ibid.

specialized systems with generic support; and the capability to ensure strategic delivery and direct support.[582]

Basic thinking must change. Information capabilities must become the basic component of a core logistic support capability; building an integrated SoS logistic operation must become an imperative; and enforcing integrated planning and military-civilian development must become the path to take. Logistic support capabilities must expand to support integrated joint operations and diversified military actions. Four principles must be adhered to: scientifically coordinating high-end planning; comprehensive integration; leapfrog advances; and effective military-civilian integration. Rapid response training, training in complex electromagnetic environments, and strategic and campaign power projection training must become priorities.[583]

On Training Modes of Information-System-Based System of Systems Operations Capability

Chinese analysts expect future warfare to be characterized by a confrontation of systems. Shijiazhuang Army Command Academy instructors Senior Colonel Wang Shulin, Colonel Zhang Yingjie, and Major Jia Chunjie discussed turning the systems training approach into a point of growth and a multiplier for combat capabilities in order to emerge victorious in a systems confrontation. Success also requires that the people's subjective initiatives be combined with scientific methods and means. Stand-alone systems of various branches of service must be merged and combat forces must be linked into the same training process.

Training objectives include turning all component parts of the information system into an organic whole and ensuring that information system users can operate information systems.[584] Commanders and forces are

> Trained to make full use of the real-time, detailed, and accurate intelligence information and the intelligent information system to exercise micro-control and elaborate coordination over such concrete nodes as specific times, places, and forces, directly command and control the endpoints of the information system through making operational decisions, shift operational actions from extensive macro-control to elaborate micro-control, and thus unleash the operational efficacy of all participating forces to the maximum.[585]

The authors also recommend organizing a strategic system of integrated training for strategic commanders, command organs, and strategic groups. Priority lies with training command personnel, staff personnel, and professional technological

582 Gao Dongguang and Wang Youlin, "A Study on Improving Core Logistical Support Capability in Information-System-Based System of Systems Operations," *China Military Science*, No. 5 2010, pp. 47-51.

583 Ibid.

584 Wang Shulin, Zhang Yingjie, and Jia Chunjie, "On Training Modes of Information-System-Based-System of Systems Operations Capability," *China Military Science*, No. 5 2010, pp. 52-61.

585 Ibid.

personnel.[586]

A Study of the Application of Nuclear, Biological, and Chemical Defense Forces Based on Information Systems

Senior Colonel Hu Xiaoping, Lieutenant Colonel Wu Guoqing, librarian Huang Yanwei, and Major Lu Xin, all from the Chemical Defense Command Engineering Academy, wrote on the issue of nuclear, biological, and chemical (NBC) defense (US doctrine now utilizes the CBRN or chemical, biological, radiological, nuclear acronym). They recognize that something as serious as a nuclear electromagnetic pulse attack could damage, if not destroy, system nodes or paralyze a system's structure. Further, the use of NBC options by an adversary could cause significant damage to what may be the primary target of such attacks, the command and control system.[587]

Disrupting communications limits a unit's ability to integrate and coordinate properly during NBC operations. These operations also disrupt vertical and horizontal linkages and limit troop maneuverability. The threat of an NBC attack encourages further improvements in friendly reconnaissance and early warning, detection, command and control, and precision strike systems. Threats also encourage the development of closer military and civilian relations.[588]

Issue 5 Summary

As in Issue 4, a variety of institutes—the Shijiazhuang Army Command Academy, the Academic Research Department of the General Logistics Department, the Naval Command Institute, and China's National Defense University, among others—discussed the SoS operational construct in Issue 5 of *China Military Science*. One set of authors noted that the SoS operational concept's guiding principle was active network defense, but they also added that (1) active offensive operations are used to achieve a defensive goal and (2) intrusion methods must be studied during peacetime to hide attacks in enemy systems. Another author wrote that the extended depth of the modern battlefield requires a greater integration of assets and the expanded use of space support. Attaining electromagnetic control is a key to success. A national defense communication system must be created. Other authors stressed the need for developing superior stratagems and establishing battlefield control as the crucial link in using and implementing operational command capabilities. Topics of discussion also included SoS's impact on political, logistic, and NBC issues.

Issue Number 1, 2011

Issue 6 of 2010 did not contain any reference to SoS type articles. However, *China Military Science* Issue 1 of 2011 contained six articles on the concept:

---

586 Ibid.

587 Hu Xiaoping, Wu Guoqing, Huang Yanwei, and Lu Xin, "A Study of the Application of Nuclear, Biological, and Chemical Defense Forces Based on Information Systems," *China Military Science*, No. 5 2010, pp. 62-66.

588 Ibid.

Issue 1, 2011

Theme Forum: Theoretical Research on Systems Operations Based on Information Systems (III)

1. "An Explorative Study of the Laws in Developing Capabilities for Systems Operations Based on Information Systems"
2. "A Study of Basic Issues on Systems Operations Based on Information Systems"
3. "A Technological Perspective on Capabilities for Systems Operations Based on Information Systems"
4. "Thoughts on Building Military Force Structure Based on Information Systems"
5. "A Study of Basic Issues on Systems Integrated Training Based on Information Systems"
6. "A Guidance for Mobilizing Capabilities for Systems Operations Based on Information Systems"

Conclusions

The topic of SoS has continued to be published and discussed in newspapers and scattered journals. It is a mainstream concept that has entered military exercises as well. But the concept has nearly disappeared from *China Military Science*. Issues 2-5 of 2011 did not mention the topic, while Issue 6 2011 and Issues 1-3 2012 each carried one article on "information systems." Other major themes, in particular those on Hu Jintao thought and advanced military culture, apparently took the place of the SoS discussion in *China Military Science*.

From the open press it is obvious that the essence of the concept was designed to reduce the fog of war, institute a new quality fighting force, take advantage of the multiplication effect that a SoS construct offers, and offer the benefits of total integration of systems of all types. Stratagems have not lost their utility and subcomponents of the military's SoS concept remain vital to future war victories: reconnaissance, early warning, sensors, control, and precision attack. Of equal if not greater importance was the focus on offensive operations as a key component of active defense. Authors noted that offensive activities will be used in preemption operations to gain the initiative in future war. Clearly the PLA has established a focus on SoS operations similar in concentration to their focus on inform-atization issues of the past several years.

While the intense discussion period ended in *China Military Science,* its continuation in other periodicals indicates that the PLA is intent on implementing the concept in the shortest possible time frame. It will be well worth the effort to continue to follow the issue in the Chinese press and see where it leads. The answer to the question "Are the Chinese merely playing catch up or instituting a different comprehensive conceptual SoS model?" appears to be that the Chinese are doing both. For sure, they were behind and are in a catch up phase even as this is written. However, as Yang Lin noted earlier, "the great difference lies in capabilities and objectives because

the development strategies and the military, economic, and technological capabilities of each country are different." In this case, innovation, creativity, and time are all on the side of the PLA as it attempts to construct its SoS configuration. As the Chinese have noted on several occasions, in confrontations on the future battlefield, what is scarier than inferior technology is inferior thinking.[589] They are working hard on both the cognitive and the technical aspect of the SoS concept to limit fears in both areas.

589 Deng Yifei, "Realizing a Historic Leapfrog in a Military Thinking Mode," *Guangming Daily*, 17 January 2008.

CHAPTER TEN
BEYOND CYBER:
CHINA'S NEW CONCEPT OF WEAPONS AND NEW CONCEPT WEAPONS

On the future battlefield, as soon as new concept weapons are put into use in large numbers, whoever uses them will be able to attack the enemy at will, unexpectedly and stealthily, at times and in places the adversary cannot imagine, causing the adversary to suffer unimaginable losses.[590]

Introduction

In addition to cyber issues discussed frequently in the Chinese press, Chinese scientists are working on what they term "new concept weapons" (NCW). These weapons include directed-energy weapons, genetic weapons, electromagnetic launch weapons, and laser weapons, among others. For example, the Chinese have studied several aspects of rail gun technology to include its load characteristics, magnetic properties, pulsed power needs, electromagnetic stability issues, and basic effects on electronic warfare and missiles. Several People's Liberation Army (PLA) universities of science and technology are involved in the research. In the US the term "electric fires" is a developing field of study that appears to fit the electromagnetic aspect of this Chinese concept.

A 2005 article in *China Military Science* placed some NCW in a category of "soft" destruction weapons. The list of weapons included laser blinding weapons, non-coherence weapons, and chemical incapacitating agents. These soft destruction weapons not only reduce casualties and environmental destruction, but also can weaken an opponent's operational capacity without the use of firepower. Countries throughout the world are allegedly studying how to develop these and other types of new weapons, according to the article.

This chapter examines NCW in general and explains how they are shaping the PLA's visualization of future war. NCW indicate that China is indeed thinking beyond cyber issues.

A New Concept of Weapons and New Concept Weapons

There has been a Chinese focus over time on two evolving concepts of weaponry. Authors Qiao Liang and Wang Xiangsui described the first concept, "a new concept of weapons," in their 1999 book *Unrestricted Warfare*. These weapons were defined in the following manner:

> New concept weapons differ from a new concept of weapons. The latter include stock market crashes, computer viruses, and rumors or scandals as

590 Song Huawen and Geng Yandong, main editors, *Informatized Weapons and Their Use*, National Defense Industry Press of China, 2010, p. 312.

new weapons. A hacker in general and a non-state actor in some instances can help create trade war; financial war; new types of terror warfare; ecological, psychological, and smuggling war; media, drug, network, and technological war; and fabricated, resource, culture, and international law warfare.[591] Technology is no longer the main factor. A new concept of weapons implies using things that initially benefit mankind to harm mankind.[592]

These "kinder weapons," the authors note, may try to paralyze or undermine, but they do not intend to produce casualties. They may compose a watershed between the old and new weapons of war.[593] Qiao and Wang state that almost any new development can become a weapon of sorts today: thus, China's awareness of how new developments can be applied must expand.[594] For example the so-called "Internet of Things" (IOT) is a research effort to enable networks that can not only connect people but can also realize communications between objects.[595] China's military is studying how to apply the IOT to joint operations and support systems in order to raise the operational capabilities of units. The focus is on combining battlefield situation perceptions, intelligence analysis and assessments, and operational processes and control mechanisms to pierce through the fog of war. This will bring about the coordination of all systems and elements. The IOT is one of the five major emerging state strategic industries in China. It is also hoped that the IOT will provide:

- An all-dimension early warning system that makes up for shortcomings in satellite, radar, and other long-range reconnaissance equipment
- The use of nanobiosensors and other sensing technologies in the development of a nuclear, chemical, and biological weapon monitoring network system
- The further application of high-speed logistic systems and real-time medical support.[596]

The development of an IOT capability is important for the military and is expanding in the civilian field as well. Recently the China Aerospace Science and Technology Corporation set up the Academy of Applications of the Internet of Things Technologies. It is hoped that the academy will create a competitive IOT enterprise that can drive the industry's development. It is a move designed to better fulfill political, economic, and social responsibility.[597]

591 Qiao Liang and Wang Xiangsui, *Unrestricted Warfare*, Pan American Publishing Company, Panama City, Panama, 2002, pp. 38-43.

592 Ibid.

593 Ibid., p. 20.

594 Ibid., p. 16.

595 "University of Macao's Internet of Things Project Included in China's 973 Program," *Xinhua* (in English), 8 November 2010.

596 "Internet of Things: Making Big Steps toward Battlefields," *Jiefangjun Bao* Online, 9 December 2010, p. 12.

597 Yang Lei, No Title Given, *Zhongguo Hangtian Bao* Online, 24 February 2012.

The second evolving concept of weaponry, dubbed NCW, includes man-made earthquakes, tsunamis, and other weather disasters, subsonic waves, new biological and chemical weapons, kinetic-energy weapons, directed-energy weapons, subsonic weapons, geophysical weapons, solar-energy weapons, meteorological weapons, and genetic weapons. Genetic weapons can harm people by attacking their biological inheritance. Computer viruses and meteorological weapons are two other examples of NCW as are incapacitating weapons, which can blind combatants or cause psychological barriers.[598]

NCW contain many information-age characteristics. They employ a greater technical domain and offer a broader set of operational targets and dramatic results than traditional weapons. A broad definition for NCW is "a class of new weapons with working principles and kill mechanisms that differ from traditional weapons, that possess unique operational efficiency, and that are currently being developed or are not yet used extensively on the battlefield."[599] Author Du Chao, writing in *Zhongguo Guofang Bao* Online, stated that new concept weapons will have an impact on the evolution of informatized warfare, as well as on the form of future war.[600]

Each NCW has unique operational principles. Instead of bullets these weapons shoot beams of light, particle streams, and electromagnetic beams. They require little or no calculation for trajectory and there is no need to calculate lead time when attacking moving targets. They propagate in a straight line at the speed of light. NCW have three methods of flight: rocket acceleration, electromagnetic acceleration, and electric heating acceleration.

There are four types of NCW according to authors Song Huawen and Geng Yandong, authors of the book *Informatized Weapons and Their Use*:

- Directed-energy weapons, such as lasers, high-powered microwave, particle beam, and sound energy weapons;
- Kinetic energy weapons, such as energy intercept and electromagnetic launch weapons;
- Hypersonic weapons, such as cruise missiles and space combat flight vehicles;
- Nonlethal weapons, such as space environment, personnel, anti-equipment, and material weapons.[601]

NCW open up new combat areas, create new deterrence measures, and establish new military advantages for those who possess them. Improvements to combat capabilities include weapons that can exert an influence on offensive and defensive space confrontations, information confrontations, and military defense and air defense

598 Song and Geng, pp. 298-299.

599 Ibid., p. 297.

600 Du Chao, "New Concept Weapons Are Set To Become New Focus in Winning Futuristic Warfare," *Zhongguo Guofang Bao*, 3 June 2010, p. 1.

601 Song and Geng, p. 300.

combat. These capabilities are essential, authors Song and Geng note, for future informatized wars. New combat forms include hypersonic technologies that lower intercept misses to practically zero and that travel at five times the speed of sound. Such characteristics make it next to impossible for defenses to be prepared to thwart attacks.[602]

It is expected that these NCW will inevitably give birth to a new military arm or service in various military powers. When NCW are used on the battlefield, actions will be speedy and stealthy. There will be little or no defense warning time. Some NCW, such as genetic weapons, microorganisms, light, and computer viruses, evade reconnaissance and observation completely. Many have no sound and no observable external form. Since NCW have such long reach they can be deployed in the campaign or strategic rear. Three characteristics in particular, which are NCW's broadened combat domain, expanded target attack range, and expanded attack channels, set the stage for a devastating fight in future wars.[603]

Electromagnetic Launch Weapon or Rail Gun

The PLA intends to use the light speed of electromagnetic launch (EML) or rail gun (used hereafter) systems to offset air defense and ballistic missile threats. The PLA is actively studying the effect of weather and other issues on rail gun parameters to insure that the weapon reaches its maximum efficiency capability. Rail gun weapons are a type of kinetic energy weapon, as noted above. They direct electromagnetic waves at targets and are considered often for their potential application as air defense weapons and as counters to cruise missiles. The experiences of the US military in their recent wars in Iraq and Afghanistan have most likely focused the PLA's attention on two areas: airpower and cruise missiles. It was not lost on the Chinese that airpower and cruise missiles represented the opening salvos of these recent wars.

In February 2011 Zhang Shiying, a senior engineer at the PLA's Naval Equipment Research Academy, offered an analysis of rail guns, citing the US naval experience with them. He stated that an electromagnetic or rail gun "uses electromagnetic force" (the Lorentz force) to fire a projectile along a rail track. It consists of an energy source, an accelerator, and a switch. The energy source uses a set of batteries that can store from 10-100 megajoules (MJ) of energy. An alternate energy source can be found in other devices as well (magnetic flux compression device or a unipolar generator). The accelerator converts electromagnetic energy to kinetic energy. The projectiles speed is Mach 5 or better and the muzzle kinetic energy reached is 33 MJ. The gun can be used to destroy satellites and intercept ballistic missiles, offering unparalleled advantages in tactical and technological capabilities.[604]

Zhang surmised that the rail gun will be a revolutionary milestone in the developmental history of weapons and equipment. Based on the size and weight of the

602 Ibid., pp. 309-310.

603 Ibid., pp. 310-312.

604 Hou Yaming, "Expert: US Military Electromagnetic Rail Gun May Become an Ultimate Weapon to Rewrite the Future Warfare Operation," *Keji Ribao*, 16 February 2011.

gun, it is expected that the Chinese Navy will be the first to use them due to the size of its platform. The gun's strategic value comes from its ability to attack some near-space operational platforms of any potential adversary. Some problems do exist, however. They include the ability of manufacturers to develop barrel materials able to withstand 3-4 million amperes of current, the ability to supply pulsed power, and the problem of overloading the resistance aspect of a related guidance control device.[605]

In July 2011 the forum *Renmin Wang* published an article on hypervelocity electromagnetic guns. The article's opening paragraph stated that an experimental gun, more advanced than those in the US, will be tested soon. Perhaps this test has already taken place, since it was also noted that:

> In August 2011, the PLA tested this hypervelocity electric gun for the first time at an artillery range in Inner Mongolia. A 25-kg projectile was launched toward a pre-determined area 250 kilometers away. The test was a success. Chinese designers are now making improvements to the hypervelocity electric gun. The effort is focused on increasing the launch weight of the projectile in order to reach the level of launching a guided projectile more than 50 kg in weight. [606]

China reportedly worked on such guns in the 1980s and has continued to work on them ever since. A breakthrough occurred in 2001 when a high-temperature superconductivity thin film was developed and applied to electromagnetic fields. This resulted in rapid advances in hypervelocity electric guns in China and apparently in testing in 2011. [607]

These guns will be supplied not only to the army, navy, and air force but also to space forces. A space-borne geomagnetic rail gun is reportedly being developed. The *Renmin Wang* article stated that electric guns can be divided into two categories, electromagnetic guns and electric thermal guns. The former can propel projectiles at 50 km per second and they are divided into three categories: rail guns, coil guns, and reconnection guns. Electromagnetic guns function as strategic weapons. Electric thermal guns can attain a launch velocity of 3 kilometers per second and are tactical in nature. There are two types of electric thermal guns: direct heating and indirect heating. China hopes to be the first to possess hypervelocity kinetic energy weapons, which were in their final testing stage in 2006, according to the article.[608]

The Work of Wang Ying

The *Renmin Wang* article also praised the work of US scientist Dr. Harry Fair. It was reputedly Dr. Fair's work that inspired Chinese scientist Wang Ying in 1981 to

605 Ibid.

606 Unattributed article, "Revelation of Latest Explosive Military Secret—Hypervelocity Electromagnetic Gun Developed in China," *Renmin Wang*, 25 July 2011.

607 Ibid.

608 Ibid.

make the subject his life's work. Wang has since coauthored two textbooks on the topic. A sampling of Wang's work includes the following: *Principles of Electric Guns* (1995); *Principles of New Concept Weapons* (1997); *The Physics of Electric Launch* (Book 1, 2004); *The Physics of Electric Launch* (Book 2, 2004); and *The Science and Techniques of Pulsed Power* (2009).

Wang writes that electromagnetic weapons refer to a weapon group fully or partially utilizing electromagnetic energy. He wrote that of the ten scientific technologies associated with future development, five are associated with electromagnetic weapons: robots, new-type batteries, artificial intelligence techniques, optoelectronic information techniques, and wireless energy transmission techniques. Further, he stated that there are five categories of electromagnetic weapons: electromagnetic kinetic energy weapons, electromagnetic pulse weapons, artificial intelligence weapons, information weapons, and electromagnetic disabling weapons.[609] Each has its own specific type of weaponry, as noted here:

- Electromagnetic kinetic energy weapons: electromagnetic guns, electro-thermal guns, various mixed electric guns, electromagnetic chemical launchers, electromagnetic catapults, electromagnetic armor, and particle beam weapons.
- Electromagnetic pulse weapons: microwave guns, microwave bombs, electromagnetic pulse bombs, electromagnetic "missiles," nuclear electromagnetic pulse weapons, millimeter wave ray guns, electronic countermeasures, electromagnetic interference transmitters, electrically pumped CO2 laser weapons, quasi-molecular laser weapons, free electron laser weapons, and electric pump X-ray laser weapons.
- Artificial intelligence weapons: robots, unmanned aerial vehicles, various missiles, intelligent landmines, and intelligent munitions.
- Information weapons: computer virus weapons, unmanned scouts, military satellites, and various radars.
- Electromagnetic disabling weapons: electro-conductive fiber bombs, photoelectric guns, light guns, electrically-powered acoustic weapons, and electrically-controlled metal storms.[610]

The *Renmin Wang* article noted that research on electromagnetic launch weaponry had been initiated in the 1980s. Papers presented at conferences some twenty-five years later indicate that much research has transpired on the topic. At the 14th International Symposium on Electromagnetic Launch Technology in June 2008, numerous Chinese authors delivered papers on electromagnetic launch technologies. These papers, whose titles were translated into English for the conference bulletin, included the following:

609 Wang Ying and Jiange Zhang, "Electromagnetic Launch Leading to Electromagnetic Weapon Era," paper provided to the author by LTG (retired) Wilson Shoffner, August 2010.

610 Ibid.

- Analysis and Optimization of Thrust Characteristics of Tubular Linear Electromagnetic Launchers for Space-Use
- Experimental Investigation of Pseudo-Liquid Armatures with Air-Springs for Rail Guns at Zero Speed
- Research on Inter-Stage Coupling of Three-Stage Reconnection Electromagnetic Launching System
- Thrust and Thermal Characteristics of Electromagnetic Launchers Based on Permanent Magnet Linear Synchronous Motors
- Section Crossing Drive with Fuzzy-PI Controllers for the Long Stroke Electromagnetic Launcher
- Design of a 3-M-Long Electromagnetic Launcher
- Evaluation of a Solid Armature's "In-Bore" Position, Velocity, and Current Distribution Using *B*-Dot Probes in Rail Gun Experiments
- The Thrust Characteristic Investigation of Double-Side Plate Permanent Magnet Linear Synchronous Motors for EML
- Simulation and Optimization of the Multi-Stage Reconnection Electromagnetic Launcher
- Analysis of Electric Parameters of a Pulsed Power Supply (PPS) System and its Influence on Muzzle Velocity in Electromagnetic Rail Guns
- Study of Employing Rail Guns in Close-in Weapon Systems[611]

One is unable to ascertain with certainty the Chinese claim as to when EML research began.

In addition to the eleven papers listed here, there were also three Chinese papers on coil launchers, two papers on pulsed power supplies, and one paper each on chemical launchers and the characteristics of projectiles.[612] The article on space use of EML indicates that this strategic weapon may be more advanced than previously thought. Thus, the study and application of electromagnetic launch technology continues to progress in China and is worthy of nearly as much research and interest on the part of US analysts as are cyber issues.

Electromagnetic Pulse Weapons (EMP)

Gao Yuliang, a professor and Director of the Radar Countermeasures Research Center in the Information Confrontation Department at the Chinese Air Force's Radar Institute, stated during a 2011 interview that "if we are to boost our deterrence in electromagnetic space, we must develop electromagnetic environment weapons, including electromagnetic pulse bombs and high performance microwave weapons."[613]

611 *IEEE Transactions on Magnetics*, January 2009, Part II of Two Parts, Volume 45, Number 1, pp. 213-218.

612 Ibid.

613 Xia Xiaosheng and Zhang Xuefeng's interview with Gao Yuliang, "Decoding Future Electronic Warfare," *Zhongguo Kongjun*, 1 July 2011, p. 35.

This also requires the establishment of a system of systems destructive attack and a reliance on the informatization of combat operations systems to bring about improvements in the integrated network and electronic warfare (INEW) information operations capabilities.[614] The objective is no longer to use immense destructive power, but rather "to achieve unprecedented accuracy and real-time management and control of operations."[615]

China, according to a *Taipei Times* report, is developing EMP weapons "in the event of a conflict with Taiwan."[616] Taiwan takes the EMP threat from China seriously. Yet its leaders did not protect its Ministry of National Defense's new headquarters from EMP countermeasures, an oversight that is often pointed out to today's leadership. Taiwanese experts point to works such as the 2004 Chinese book *EMP and EMP Protection* as a cause for their concern. Written by Zhou Bihua, the book has an English Table of Contents. Only the main chapter headings are listed here.

- Chapter One: Effects of a Nuclear Weapon Explosion and Electromagnetic Pulse
- Chapter Two: Nuclear Electromagnetic Pulse Environments
- Chapter Three: Coupling of Nuclear Electromagnetic Pulses
- Chapter Four: Effects of EMP on Microelectronic Equipment
- Chapter Five: Simulation Techniques of EMP
- Chapter Six: Measurement and Signal Processing of EMP
- Chapter Seven: EMP Protection
- Chapter Eight: Simultaneous Action of EMP
- Chapter Nine: High Power Electromagnetic Environments.[617]

An apparent goal of Chinese military experts working to counter enemy EMP use is to prevent the coupling of EMP weapons with electrical systems. This will be hard to do, but the extended use of optical fiber is one way to ensure this does not happen easily. It is also a worthwhile idea to build certain anti-EMP barriers into equipment as it is fielded, something the Taiwanese military apparently failed to do.

EMP and nanotechnologies are both thought of as potential "trump cards" if China can develop them quickly and utilize them with precision, such as their use against an information network or nodes. It is unknown if the Chinese are working to develop nonnuclear EMP weapons at the tactical level, but it is likely that such research is underway. Tactical-level EMP can, through the use of radiation or laser effects, greatly influence operations in future conflicts especially against information systems.

---

614 Ibid.

615 Zhang Feng, Liu Zengliang, and Lu Dehong Lu, "Systems of Military Strategy in the Information Age," *China Military Science*, No. 2 2005, pp. 90-99.

616 Vincent Chao, "EMP Defense Necessary, Legislators Say," *Taipei Times* Online, 27 July 2011.

617 Zhou Bihua, *EMP and EMP Protection*, 2004 (place of publication unknown).

Conclusion

The future electromagnetic environment will most likely be filled with variations of the research activities described above. Undoubtedly these activities will dramatically affect future conflict as these activities are operationalized. Future war will involve not only long, medium, and short-range precision guided missiles and information systems such as surveillance and reconnaissance systems, but also new concept weapons of the "soft destruction" variety. Several Chinese authors defined the impact of "soft destruction" weapons as follows:

> Soft destruction weapons such as laser blinding weapons, noncoherence weapons, infrasonic weapons, microwave weapons, nonnuclear electromagnetic pulse weapons, and chemical incapacitating agents not only strip opponents and their equipment of their expected effectiveness, but reduce casualties and environmental destruction. It is foreseeable that in the near future an enemy's operational systems could be paralyzed and his operational capacity could be weakened without the use of firepower.[618]

Seizing the initiative to control information and networks via these and other weapon varieties has become the prerequisite for the conduct of operations, according to Chinese thinking. Seizing comprehensive strategic superiority and paralyzing an opponent's strategic command systems will be the focal point for the use of these new concept weapons. Warfare will be vastly different than what humanity has experienced to date once these systems are activated.

618 Zhang, Liu, and Lu.

CHAPTER ELEVEN:
COMPARING CHINESE AND RUSSIAN CYBER CONCEPTS

Introduction

A question often posed at conferences regarding the cyber activities of other nation-states is "aren't all cyber activities basically the same since they are all based on similar infrastructures (optical fiber, wireless connections, etc.) and all utilize electron flows?" The answer to the question is an unequivocal "it depends." It depends on how much freedom is allowed to scour the Internet openly and thoroughly, on how nation-states decide to utilize the Internet's anonymous nature to conduct espionage or illegal activities online, on how countries define their cyber sovereignty, on how countries unite to influence the authorship of cyber codes of conduct or United Nation resolutions, and on how much traditional and cultural creativity and influence are imbedded in cyber methodologies and rules, regulations, and doctrines, among other issues. This chapter will demonstrate the differences and similarities in some of these practices between China and Russia and how they differ from US practices.[619]

China

China has been accused of many wrongdoings over the past several years. Currency manipulation, dumping, pollution, and illegal subsidies are at the top of the list. With regard to cyber issues, Internet Protocol (IP) theft and intrusive reconnaissance or theft of financial, military, and other sensitive systems and data are of most concern.

Different terminology. Some Chinese cyber terminology is similar to that of the US. Both countries, for example, use the term "information superiority," even though the emphasis on particular aspects of the term differs. Other terms differ more widely. For example, information control is a common concept that the Chinese use, while the US uses the term less frequently. Information control is more focused on ensuring the security of digits and on digital trustworthiness. It is one thing to have information superiority, the ability to collect and process information at will, but it is quite another to be able to control information and ensure its trustworthiness. Many other Chinese cyber concepts, however, are different either in meaning or content or both. Some cyber-related terms in the Chinese vocabulary include water army, 50 cent party, human flesh engine, system sabotage, integrated network electronic warfare, *shi*, cocktail warfare, and war engineering. Such terms do not appear in either Russian or US cyber work.

Informatization Development Strategy. In 2006 the Chinese published their State Informatization Development Strategy for the years 2006-2020. Its goals were as follows:

- Provide an information infrastructure nationwide

619 This chapter was originally a paper for a workshop at the University of California, San Diego in April 2012. A few Chinese descriptions are similar to those discussed above.

- Strengthen capacities for the independent innovation of information technology
- Optimize information industry's structure
- Improve information security
- Make effective progress in building a more information-oriented national economy and society
- Establish a new type of industrialization model
- Build a perfect national policy and system for the informatization process
- Enhance the capability for applying information technology among the public.[620]

Nine key aspects were emphasized. They were:

- Promote the informatization of the national economy
- Popularize e-government
- Establish an advanced Internet culture
- Push ahead social informatization
- Popularize the information infrastructure
- Exploit information resources more efficiently
- Improve information industrial competition
- Build a national information security system
- Improve people's ability in using information technology and cultivate more talent in information technology.[621]

The Chinese effort was six years behind the Russian effort, which started in 2000. Still, the strategy is a good step forward and provides a template for the country's future needs.

Soft power focus. In a 2005 article in *China Military Science*, author Wang Shudao noted that China must take action "to propel China's culture industry and media industry beyond China's borders in an effort to take over the international culture market."[622] This effort has taken flight. Today China is taking out full page ads periodically in *The New York Times* and in *The Wall Street Journal*. As of 2010 it had established 316 Confucius Institutes, which offer classes on the Chinese language and culture, in 94 countries across the globe. There are now virtual apps for the Xinhua News Agency in Cuba, Mongolia, Malaysia, Vietnam, Turkey, Nigeria, and Zimbabwe, among many other nations. There is an iPhone app for Xinhua news, cartoons, and financial information. Recently China's television station CCTV opened an office in

620 "China Maps Out Informatization Development Strategy," Embassy of the People's Republic of China in the United States of America," 11 May, 2006, found at http://www.china-embassy.org/eng/xw/t251756.htm.

621 Ibid.

622 Wang Shudao, "Modern Cultural Diffusion and National Security," *China Military Science*, No. 3 2005, pp. 64-69.

Washington DC and has begun broadcasting news in the US on a station known as CCTV America. Thus this intention to spread China's soft power has taken root. In this sense China's soft power initiatives have a decidedly offensive character at the present time. They feel a soft power offensive is necessary to offset the "verbal hegemony" of the West, as they term it.

System of system (SoS) focus. The topic of SoS never appeared in military journals as prominently as it did in 2010 and early 2011. From the open press it is obvious that the essence of the concept was designed to reduce the fog of war, institute a new quality fighting force, take advantage of the multiplication effect that a SoS construct offers, and offer the benefits of total integration of systems of all types. Stratagems have not lost their utility either and are still embedded in SoS thinking. Specific subcomponents of the military's SoS concept—reconnaissance, early warning, sensors, control, and precision attacks—remain vital to future war victories. Clearly the People's Liberation Army (PLA) has established a focus on SoS operations similar in concentration to their focus on informa-tization issues over the past several years. This focus on SoS continued into 2011. In the first edition of *China Military Science* for 2011 there were seven more articles on the SoS topic. They covered laws for developing SoS capabilities; basic SoS issues; technological perspectives of SoS capabilities; building a military force structure based on the SoS concept; war-fighting capabilities of SoS; SoS and integrated training; and SoS mobilizing capabilities. This effort appears oriented toward integrating hard power capabilities and producing some soft power intimidation effects during the process.

Different pace of development. It has taken China longer to obtain the necessary scientific, infrastructure, and monetary capabilities to put together a significant space or cyber threat. The nation now has many of those capabilities and can begin to think about moon missions and other geospatial endeavors. China has launched a rival to the US global positioning system (GPS) with its Beidou Navigation Satellite System. It is working hard on developing an "exascale" computer by 2020 that can deliver 500 times the computing power of the present US Sequoia computer (with the ability to deliver 20 quadrillion operations a second). The Chinese are working hard on developing a first-rate quantum computing capability as well.

Different methods and tactics. Fang Binxing, the father of China's "great firewall," stated that "the weaker party can only overcome its opponent by utilizing tactics different from its opponent."[623] Two people engaged in martial arts cannot mimic one another.[624] One of these tactics could be "cocktail warfare," a concept developed in the 1999 book *Unrestricted Warfare*. One of the book's authors, Qiao Liang (a colonel at the time in the PLA), wrote that new concepts of weapons involve the ability to combine various elements to produce types of weaponry never imagined before. For example, Qiao may be referring to combinations such as "cyber preemption + network reconnaissance +

623 Fang Binxing, in Richard Suttmeier and Xiangkui Yao's report *China's IP Transition*, The National Bureau of Asian Research, Special Report #29, July 2011, p. 22.

624 Ibid.

high-technology deception + financial market disruption + network deterrence" to produce an overall effect and a new weapon. In January 2012 Qiao stated that China must "make trouble for the trouble makers" (meaning the US). The unrestricted war he recommends is "not mainly tactics but a mode of thinking." Further, he states that the weaker side (China in his view) does not have to abide by regulations formulated by the superior side.[625] Qiao is now a Major General in the PLA, so his views take on more importance than when he was a colonel.

Another tactic is using packets of electrons as stratagems. A stratagem is designed to mislead enemy processes of perception, thinking, emotion, and will. In this case, packets of electrons could be used to fulfill stratagems such as "rustle the grass to startle the snake" (throw thousands of pings at a site until it becomes clear where firewalls pop up).

Physical infrastructure. According to one Chinese source, China Telecom, China has three international transmission management centers that manage incoming foreign digits. Telecom's website describes two submarine cable landing stations, two satellite stations, and numerous nodes around the country that serve as terrestrial cable gateways. It is believed that 95% of China's Internet traffic transpires over the submarine cables, 3% over terrestrial cables, and 2% over satellite connections.[626]

Code of conduct. On 14 September 2011 China, Russia, Tajikistan, and Uzbekistan offered an international code of conduct for information security for the United Nations' consideration. The code noted that efforts should be directed at providing developing countries with information technology, that operations consistent with the objective of ensuring Internet stability is required, and that policy authority for Internet-related public issues is the sovereign right of States. The latter issue is of particular concern to the US State Department, since it implies that citizens of these countries will not have full access to the Internet, but only to those portions deemed essential by China, Russia, and the others. A few of the key portions and pledges of the text include:

- To not proliferate information weapons
- To respectfully comply with the diversity of social systems of all countries
- To endeavor to prevent other states from undermining the right of countries that have accepted the code of conduct
- To reaffirm the rights of states to protect their information space from disturbance
- To respect rights and freedom in information space on the premise of complying with relevant national laws and regulations
- To promote an Internet management system that facilitates access for all
- To lead all elements of society to understand their roles and responsibilities

625 Qiao Liang, "'War and Peace' Are No Longer Limited to the Military," *Nanfang Zhoumo* Online, 4 January 2012.

626 Mr. Scott Henderson, FMSO, found and offered this information to the author.

with regard to information security.[627]

The key questions regarding the code are "which of these points take priority" and "how are States to interpret statements like 'protect information space from disturbance'?" What is considered to be "disturbance," that is, is a free and open Internet a "disturbance"? Is it okay to respect the rights and freedom of information space or will the requirement not to proliferate information weapons (which was not defined) take precedence and limit some states understanding of rights and freedoms? One Chinese article noted that the difference between the code of conduct and its European and American counterparts is that China and Russia believe that "the flow of information should not be used to compromise the sovereignty of a sovereign state."[628] A detailed examination of what is considered information sovereignty and other such concepts is required before any Western nation would agree to the code of conduct as it is presently written.

The Concept of Information Deterrence (for China's concept, see pages 39-55 above)

Russia

Russia is one country that has been at the forefront of preparing United Nations resolutions on information security, doing so since 1995. The primary reason for this focus is undoubtedly the loss of an ideology in 1989, when the Soviet Union dissolved. Russia has continued to do well in the technological arena. The country has a multitude of resourceful cyber code writers who have continued to keep the nation close to the top of those writing computer viruses or in the prevention of cyber assaults.

Impact of the loss of ideology. As a result of the loss of communist ideology, a principal focus of the Russian leadership has been on maintaining control of the flow of information in the country and its impact on the conscience of the citizenry. Some still blame the fall of communism on an information-psychological assault from the West. This focus has manifested itself in the Russian definition of information warfare, forcing it to include both technical and psychological aspects in its definition of the term. Russia thus looks at soft power issues more closely than most countries. It worries about people like Alexei Navalny, the anticorruption blogger who orchestrated many of the demonstrations against Prime Minister Vladimir Putin's run for the Presidency. Navalny is the only opposition leader barred from state-controlled TV, and he has been characterized as a CIA operative, as Russia's leadership tends to brand people who are against them. For Navalny the Web offered a way to publicize his work on LiveJournal blog. The Kremlin will be watching his every move in the coming months as he continues to discuss corruption at the highest level in Russia.

Conceptual views and codes of conduct. As noted above, Russia was a signatory

627 "Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan, and Uzbekistan to the United Nations addressed to the Secretary-General," Sixty-sixth Session of the United Nations General Assembly, 14 September 2011.

628 Zhang Zhe, "China and Russia Spearhead to Promote Proposed Cyberspace Code of Conduct to Counter the United States," *Dongfang Zaobao* Online, 14 September 2011.

to the 12 September 2011 "Code of Conduct" letter addressed to the General Secretary of the United Nations. In 1995 the country offered definitions of information war and information weapons at the UN that were later rejected by the US. In 2000 the Russian Security Council proposed an Information Security Doctrine for the country that was accepted and implemented by the Kremlin. In 2011 the Ministry of Defense proposed a "Conceptual Views on the Activities of the Armed Forces of the Russian Federation in Information Space." The Conceptual Views document defined terms that included, as in 1995, information warfare and information weapons, among others. Conceptual Views also offered principles (legality, priority, integration, interaction, cooperation, and innovation) to guide the activities of the Armed Forces of the Russian Federation in information space. Issues that stood out include the following:

- Legality: respect for national sovereignty and noninterference in the internal affairs of other states;
- Priority: collect relevant and reliable information regarding threats, protect information resources;
- Integration: utilize a coordinated and unified system to enhance the capabilities of the entire system;
- Interaction: coordinate defense activities with other federal executive bodies;
- Cooperation: develop cooperation on a global level to detect and prevent information and technological threats to peace, settle disputes involving these assets, build confidence in regard to the use of trans-boundary information systems, and ensure the secure use of common information space;
- Innovation: recruit skilled personnel; Russia's innovation centers must be able to develop and produce systems capable of carrying out activities in information space.[629]

The Conceptual View further included rules for the use of information space (as an agent of conflict deterrence, conflict prevention, and conflict resolution):

- Deterrence and conflict prevention: develop an information security system for the RF Armed Forces that can deter and resolve military conflicts in information space; remain in a constant state of readiness; expand the group of partner states; conclude, under UN auspices, a treaty on international information security; establish control over the escalation of conflict; take priority steps to counter the development and spread of a conflict; neutralize factors leading to the conflicts spread; and shape public opinion means to limit the ability of instigators to further

629 "Conceptual Views on the Activities of the Armed Forces of the Russian Federation in Information Space," Ministry of Defense of the Russian Federation, 2011.

escalate the conflict.

- Conflict resolution: resolve information space conflicts primarily through negotiation and reconciliation; if in a crisis stage, exercise individual and collective self-defense rights not inconsistent with international law; deploy manpower and resources for ensuring information security on the territory of other states in the course of negotiations in accordance with international law; keep all media informed of the situation.[630]

The Conceptual View included confidence-building measures that should be utilized, to include exchanging national concepts for ensuring information space security, as well as exchanging information promptly about crisis events. It was noted that Russia's defense capability depends to a large extent on the effectiveness of Armed Forces activities in information space. Russia will do what it can to develop "an international information security system in the interests of the entire global community."

On the essence of cyber war terminology. One Russian author defined cyberspace as an objective reality, a medium for computer functions in which one can affect an enemy's systems and protect one's own. In cyberspace, "it turned out to be very convenient to 'wash away' the boundaries between war and peace. In fact, one can inflict damage on an adversary without formally stepping across the boundary separating war from peace."[631] A cyber attack was defined as a form of hostile actions in cyber-space aimed at cyber systems, information resources, or an information infrastructure to achieve some goal, implemented with special programs, equipment, and methods. Cyber war was defined as the systematic struggle in the cyber domain among states, political groups, and extremist and terrorist groups, where targets are information resources and whose properties (integrity, accessibility, and confidentiality) can be violated.[632] There does not exist a particular cyber lexicon that approximates China's cyber terminology.

Asymmetric opposition to network-centric warfare. Russian authors do discuss the topic of network-centric warfare (NCW) and often do so through the framework of the US use of the term. One set of authors defined the central task of US NCW as the conduct of effects-based operations. The Russians do not discuss the Chinese concept of integrated network-electronic warfare (INEW) with the same intensity. The Russians have discussed counters to the US network-centric principle. In one article, three retired officers stated that to counter NCW symmetrically three conditions must be fulfilled: creating a super-reliable communication medium to ensure the effective functioning of computer networks; implementing a spatially disbursed grouping of intelligence and command and control resources; and creating a disbursed program medium providing real time processing of information streams. Asymmetric counters to NCW were offered as well, such as the use of electromagnetic bombs, destruction

630 Ibid.

631 P. I. Antonovich, "On the Essence and Content of Cyber-War," *Military Thought*, No. 7 2011, pp. 39-46.

632 Ibid.

of an air adversary over his own territory, the use of unmanned aerial vehicles (UAVs) against cruise missiles, infrastructure strikes (such as against global navigation systems resources), heavy UAV strikes, magnetic information carriers to destroy software, and the use of weapons of mass destruction at brigade level. It is also necessary to utilize the increasing potential to disorganize an enemy command and control system. Finally, until it is possible to achieve parity in network-centric technologies, Russia must only use "manual" command and control at the tactical level, according to these three officers.[633]

The Concept of Information Deterrence. In 1996 Colonel Sergei Modestov of the Russian Armed Forces wrote one of the first Russian articles related to the topic of information deterrence.[634] Modestov did not directly define information deterrence. Instead he talked around the topic. He defined a nation's center of gravity as "those elements of each national system upon which the system's overall stability depends."[635] One nation's ability to impose threats against the stabilizing elements of another nation serves as the "strongest possible deterrent in a crisis."[636]

Modestov wrote about the growing role of the information component in regard to the nuclear issue. A nuclear weapon's precision is enhanced through its information component. Information allows for more realistic predictions and computations in the effects of guidance systems, communications and intelligence, and ways to control an opponent's weapon systems and command of troops. [637]

In addition to systems, Modestov noted in a footnote that the capabilities for influencing the human mind with information technology must also be studied. Here he included the effects of extrasensory perception capabilities, virtual worlds, and neurolinguistic programming on the human mind through the use of various applications of information technology.

For each state, then, the best geopolitical evolution of contemporary assets includes a balance among all types of resources, to include information, nuclear, and conventional forces, to prevent the overall development of a single vulnerable center of gravity. The question under conditions of information dominance is not the issue of immediate unacceptable destruction, as with the nuclear issue, but rather the effect on the nation due to lost resources and a consequent inability to use force effectively.[638]

In addition to resources, intelligence is another very important information deterrence component. Intelligence information systems provide necessary conditions for cooperation among and between states and reduce the level of nuclear confrontation. Synergistic deterrence, he noted, requires the systematic interaction of all interested states.

---

633 P. A. Dul'nev, V. G. Kovalev, and L. N. Il'in, "Asymmetric Opposition in Network-Centric Warfare," *Military Thought*, No. 10 2011, pp. 3-8.

634 Sergei Modestov, "The Possibilities for Mutual Deterrence: A Russian View," *Parameters*, Winter 1996-1997, pp. 92-98.

635 Ibid., p. 94.

636 Ibid.

637 Ibid., p. 96.

638 Ibid., p. 97.

Modestov followed up his 1996 article with another in late 2008 advocating specifically for the concept of strategic deterrence in a theater of information warfare. Again, he did not mention "information deterrence" by name but discussed information resources (IR) as the target of strategic deterrence. In particular, he noted the importance for Russia of developing "military-theoretical views on the forms of deployment of forces and assets for targeted impact on an adversary's IR for strategic deterrence purposes."[639] Operational tasks supporting this goal include disorganizing an adversary's governmental and military administrations; damaging economic potential, especially military-economic potential; and conducting intelligence operations.[640] From a Russian point of view, this leads to a strategic operation in the "theater of information warfare," the latter defined as the sum total of the following actions:

- Operations to rebuff an aerospace attack
- Strategic nuclear forces operations
- Operations in a continental theater of war
- Operations in a maritime theater of war
- An aerial operation in a theater of war[641]

Another aspect of Russia's cyber deterrence can be found in its desire to limit other nations' cyber capabilities through legal means or through the efforts of doctrine and strategy. This effort has continued unabated since the early 1990s. Some of the efforts were at the official level, some at the unofficial level. For example, *The National Security Strategy* of Russia of May 2009 listed several information-related international security tools, to include technologies, software, linguistic, legal, telecommunication channels, and organizational items as the key tools to protect in the national security system, since they are used to transmit or receive information on the state of national security.[642] The concept was divided into "The Contemporary World and Russia"; "Russia's National Interests and Strategic National Priorities"; and "Organizational, Normative-Legal, and Information Bases for Implementing the Present Strategy." Specific information issues that the document discussed included the following:

- The global information confrontation
- The use of information to enhance strategic deterrence
- The ability of information to present a threat to military security
- The illegal movement of narcotics and "psychotropic substances" [which can alter thinking and the information security of the mind]
- The preservation of information technologies and information focusing on the various issues of society's sociopolitical and spiritual life

639 Sergei Modestov, "Strategic Deterrence in the Theater of Information Warfare," *Academy of Military Science Bulletin*, No. 1 2009, p. 35.

640 Ibid.

641 Ibid., p. 34.

642 Russian Federation Security Council Website, 12 May 2009.

- The development of information and telecommunications technologies such as computer hardware and electronics
- The proper use of the information-telecommunication medium
- The implementation of a series of information measures serving as the basis of this strategy: the harmonization of the national information infrastructure with global information networks and systems; overcoming the technological lag in information science; developing and introducing information security technologies in the state and military administrative systems; increasing the level of protection of corporate and individual information systems; and creating a single information-telecommunications support system for the needs of the national security system.[643]

All of these items together help produce an integrated strategic information deterrent.

An unofficial source of information deterrence can be found in the efforts of Moscow's Lomonosov University to conduct international information conferences. For the past several years, the University has held home and away (at Garmisch, Germany) international conferences. The focus of the conferences has been on international cooperation, data protection, governance mechanisms, and cooperation in research and development. In 2010, the topic of IW deterrence was added to the agenda. In 2011 the topics included legal provisions to regulate information behavior; defining the sources of cyber attacks; development of an international information security glossary; and content monitoring and filtering.

Ten cyber topics were presented to some Russians. They were asked to rank-order the topics from the most to the least interesting. The Russians who were queried settled on the following order:

- Escalation models
- Civil infrastructures
- Definitions
- Cyber law
- Codes of conduct
- Cyber terrorism
- Cyber crime
- Technical cooperation
- Protection of the world community
- Industrial espionage[644]

643 A. A. Strel'tsov, *Gosudarstvennaya Informatsionnaya Politika: Osnovy Teorii* (*Government Information Policy: Basic Theory*), Moscow MTsNMO 2010.

644 Information obtained by the author while attending the April 2010 conference in Garmisch, Germany.

The placement of escalation models at the top of the list demonstrates that even unofficially the Russians are very interested in containing the outbreak of a cyber incident. Cyber deterrence models appear to be one way of doing so.

Finally, A. A. Strel'tsov, a co-editor of the Russian *Information Security Doctrine* that was written in 2000, listed some high-priority scientific issues related to the "Theory of Government Information Policy" and, coincidentally, to the implementation of information/cyber deterrent qualities.

First he noted that political consciousness and public opinion must be strengthened and thus are targets of government information policy. Political consciousness is a factor in society and in the stability of its development, as well as the legitimacy of the transformation of political consciousness in a historical context. Public opinion is a factor of political life in society. Legal and organizational mechanisms for government influence the development of political consciousness and the shaping of public opinion in historical and political contexts. When strengthened they become deterrents to outside attempts at influence.

Second, social institutions for education and instruction are factors ensuring the competitive advantages and stability of social development and thus are targets of government information policy. For example, religious organizations are targets in the educational and instructional system. When strengthened they too become deterrents to outside attempts at influence.

Third, information support and the role and place of the ideology of the agent holding public authority shapes and implements government information policy. This can be accomplished via legal and organizational mechanisms to counter the spread of ideologies of legal nihilism, extremism, and terrorism, especially during periods of information warfare advances (use of computers, etc.) made by these groups.

Fourth, there are important methods and means that must be developed for an information deterrence policy to be effective. These include methods and means for:

- Uncovering and evaluating threats to the implementation of government information policy brought about by the activities in the information sphere of national and foreign political forces that oppose the agent holding public authority
- Evaluating the socioeconomic and political effectiveness of government information policy measures
- Using state-of-the-art information technologies to implement government information policy
- Using the potential for international cooperation to implement government information policy
- Instituting cooperation between government officials and agencies and nongovernmental organizations and citizens in the process of implementing government information policy
- Evaluating and predicting the effectiveness of government policy in

developing political consciousness and influencing the sociopolitical and economic development of society.[645]

Conclusions

In conclusion, there appears to be more similarities than differences in the Chinese and Russian approaches. Similarities include the following:

- Both countries are signatories to the Code of Conduct;
- Both countries worry about cyber's influence on the public and continue to support State-run television networks and other media to insure control of public opinion;
- Both countries are working on GPS systems, Beidou in China and Glonass in Russia;
- Both countries have begun a focused development of new concept weapons as a source of asymmetrical counter weapons, to include electromagnetic pulse, rail guns, nanotechnology development, and so on;
- Both countries rely heavily on Marxist thought.

Differences include:

- Russia is in a soft power protection mode while China is in both a soft power protection mode and also in a strong offensive projection mode at the present time.
- Overall, the Russian side does not seem to have as many clarifying cyber terms (water army, human flesh engine, etc.) as the Chinese.
- China has not developed a concept to date for its military as the Russians have done with their "Conceptual View" document.

645 Strel'tsov, pp. 102-103.

PART FOUR
CONCLUSIONS AND APPENDIXES

CHAPTER TWELVE
CONCLUSIONS

Introduction

China and the People's Liberation Army (PLA) are making impressive gains in the cyber arena. These gains are making it easier for China to consider the use, as *Unrestricted Warfare* authors Qiao Liang and Wang Xiansui noted, of new "concepts" of weapons (computer viruses to cause a stock market crash, etc.). China's cyber weapons have found their greatest utility, however, in important data reconnaissance and theft missions. They have left behind a trail of frustrated and angry US cyber experts.

The well documented intrusive efforts of the Chinese are meeting with increased confrontation from the US. Three important US policy makers from the intelligence, homeland security, and defense fields, Mike McConnell, Michael Chertoff, and William Lynn, underscored the high-level attention this threat has received. They wrote in a 2012 *Wall Street Journal* editorial titled "China's Cyber Thievery is National Policy—and Must Be Challenged" that China is the world's most active practitioner of economic cyber espionage:

> Evidence indicates that China intends to help build its economy by intellectual-property theft rather than by innovation and investment in research and development (two strong suits of the US economy). The nature of the Chinese economy offers a powerful motive to do so.[646]

To keep economic growth alive for its inexpensive work force, China has opted to steal innovations and intellectual property rather than spend time and money on high-technology developments, the authors add. Cyberspace is the medium through which to accomplish this goal. The cost to the US economy in terms of espionage's impact on national security, jobs, and creativity is difficult to compute but surely equates to the loss of billions of dollars and millions of jobs.[647]

This chapter summarizes some of the Chinese and PLA cyber activities over the past three years. It demonstrates China's recent cyber developments and apparent unconcern with growing international tension over its activities.

2009-2011

US analysts should be concerned about the speed and direction of China's cyber efforts. There is also concern regarding the PLA's intentions. Studying US cyber policies is one thing, but attempting to find ways to exploit them is quite another. China is doing so without the legal limitations that are imposed on US cyber strategists. In short, in spite of US advantages it has several disadvantages that China is working to manipulate.

646 Mike McConnell, Michael Chertoff, and William Lynn, "China's Cyber Thievery is National Policy—and Must Be Challenged," *The Wall Street Journal*, 27 January 2012, p. A15.

647 Ibid.

There is a strong Chinese focus on soft power or the use of information to persuade other nations of China's peaceful intent. In this sense, China continues to spread its influence through the guise of acting as a peacetime activist. The reason that activities such as deterrence and deception are more successful than in the past is due to the properties of the Internet and the digital age. Issues, to include cultural proclivities, are spread faster and farther and reach a much wider audience than in the past. Wartime targeting is enhanced by having sampled a population's feelings and rationale via the net in peacetime. Several Chinese media experts even believe that at the strategic level there is no difference between peacetime and wartime media. In both cases there are attempts to affect the subjective judgment of members of a society. The use of multiple sources can add weight to the process of convincing individuals or groups of a concept.

Soft power efforts represent the continuous development of a strategic, integrated, and comprehensive cyber capability to persuade. The rapid growth of these elements could imply an overall effort to impose an "information deterrence" stranglehold on the US. The 2004 Chinese book *New Concepts during Military Transformation*: *Interpreting 200 New Military Terms* defined several deterrence-related terms, to include the strategy of deterrence, strategic deterrence, nuclear deterrence, space deterrence, forward deterrence, full spectrum deterrence, and, most importantly, information deterrence. The latter term was defined in the following way:

> With the backing of information weapons, intimidating and containing an adversary by threatening to use information weapons or when necessary carrying out an information attack. Information deterrence is essentially warning an adversary in advance about the possibility that information weapons will be used or information attacks will be carried out, as well as the serious consequences these actions may give rise to, causing the adversary to weigh the pros and cons and thereby producing psychological fear, forcing him to submit to the will of the side carrying out deterrence or abandon his original plans and thus allowing the side carrying out deterrence to achieve certain political objectives.[648]

In 2009, Central Military Commission member General Jing Zhiyuan stated that in the 21st century, strategic deterrence must be built up with the construction of "information-technology-dependent strategic missile forces."[649] The implication here is that the amount of information technology built into modern systems indicates the deterrent capability of China's strategic force.

A reorganization of Chinese cyber capabilities is indicative of the renewed focus on digital issues of both soft and hard power. Recently the PLA has established several new organizations as part of its cyber reform effort. These organizations include the creation

---

648 National Defense University's Scientific Research Department, *New Concepts during Military Transformation: Interpreting 200 New Military Terms,* PLA Publishing House, 2004, p. 108.

649 "'Strategic Deterrence' Enhanced in the Information Age, Top Nuke Generals," *Xinhua*, 2 February 2009.

of a cyber-based headquarters or center responsible for tackling potential cyber threats and safeguarding national security, announced in 2010. A general staff officer stated that "the base just means that our army is strengthening its capacity and is developing potential military officers to track information-based warfare."[650] An informatization department in the general staff was created on 30 June 2011 and announced in early July. A *China Daily* report noted that the Communication Department of the General Staff was to be restructured and renamed the Informatization Department. The announcement mentioned that this was a new step toward developing further the requirements for an information-based PLA and would affect communication units at corps level and above.[651] The construction of a Blue Force ensures that the PLA is becoming more and more familiar with Western doctrine and equipment. More importantly, the Blue Force allows the PLA to finally, after years of scripted fighting, work against a realistic opposition force (OPFOR) on potential future battlefields.

Finally, the establishment of a Strategic Planning Department signifies a serious PLA effort to envelop traditional and cyber-related war-fighting capabilities, plans, and policies into a united effort. The department is designed to serve as a key think tank for the Central Military commission. Its job is to coordinate the strategic planning of the armed forces, optimizing their allocation, distribution, and integration, and to look ten steps ahead to eliminate blind or random decision making. This helps the PLA to win a war before it starts. The department meets the needs of facing systemic operations and information warfare challenges.[652]

China is also an intelligence activist, utilizing electronic reconnaissance at every opportunity to gather information on potential opponents. Two conceptual issues from Chinese military history are at work here that appear to influence the PLA's cyber behavior. They are virtual *shi*, or efforts to attain a strategic advantage in the cyber world; and information control, which is working hard to pass in importance the concept of information superiority in China. If one is able to attain strategic advantage through planting viruses such as the Trojan horse or spotting vulnerabilities in Western systems via reconnaissance activities, then it is possible to activate destructive codes at a time of China's choosing. Knowing a system's weakness ahead of time helps attain the initiative in future battles. It is no secret that the Chinese have conducted extensive reconnaissance activities of US and UK systems, among other nations', over the past several years. Google, the Pentagon, and other key facilities have all purportedly been penetrated.

Control is also an aspect of China's attack planner philosophy. One PLA author stated that to control war in the initial stage of combat the active offense must be emphasized. To win local wars under informatized conditions, the PLA must employ control warfare along with information warfare, firepower warfare, and mobile warfare,

650 Peng Pu, "PLA Unveils Nations First Cyber Center," *Global Times* Online (in English), 22 July 2010.

651 Zhang Yanzhong and Li Qiang, "GSH Communication Department Restructured into an Informatization Department," *Jiefangjun Bao* Online (in English), 1 July 2011.

652 Luo Yuan, "Setting Up the PLA Strategic Planning Department is a Move Up the Strategic High Ground," *Zhongguo Qingnian Bao* Online, 2 December 2011.

to include countermeasures.

Authors Zhang Yu, Liu Sihai, and Xia Chengxiao stated that a "post-emptive" move is "not an effective way to seize the initiative on the informatized battlefield." To seize the initiative and control war in the initial state of conflict, the active offense must be emphasized. That is, when signs of enemy invasion are clear, then China should seize "early moments of opportunities to dominate the enemy" through offensive operations which cannot be separated from active defense. Guidelines offered for controlling war include establishing favorable conditions in the opening of war, placing equal emphasis on deterrence and combat, grasping the center of gravity of war, destroying and attacking systems, strengthening the interactions between combat systems and war systems, and ending war as early as possible by combining fighting with negotiations.

Several other PLA authors agree that an attacking capability is a key factor in influencing the outcome of war. For example, China's well-known cyber expert, retired General Dai Qingmin, has an entire section of his 2008 book *New Perspectives on War* dedicated to "attacking combat systems." It is necessary to paralyze an enemy's financial, transportation, telecommunications, and power systems, Dai writes. The paralysis of an opponent's strategic command system introduces deterrence as well.

The Chinese write that the Western "system of systems (SoS)" issue is an attack planning option as well. PLA members write that the concept was designed, from their vantage point, to reduce the fog of war, institute a new quality fighting force, take advantage of the multiplication effect that a SoS construct offers, and offer the benefits of total integration of systems of all types. The SoS concept appears to be a key component of their attack planner concept, especially when discussing network issues. For example, authors Li Daguang and Han Yufeng state that the theory has offensive aspects, to include attack software (with paralysis, obstruction, and deception applications). Offensive operations are easier to conduct than defensive operations, with a cost effectiveness ratio of 1:100. Further, the authors note that it is necessary to launch offense as defense, and use active offense operations to achieve defensive results. Offensive counterattack forces must be maintained in case of a surprise attack.

These offensive developments utilize and are buttressed by updated versions of several older concepts. For example, stratagems such as "win victory before the first battle" are mentioned as an implied cyber goal of the Strategic Planning Department. By successfully planting viruses or uncovering vulnerabilities in US systems the PLA is able to fulfill this stratagem. Stratagems have not lost their utility for the SoS concept either, as subcomponents of the military's SoS concept, to include reconnaissance, early warning, sensors, control, and precision attack remain vital to future war victories. There are also cyber mobilization exercises associated with SoS concepts, which are intended to increase the capabilities of the information industry and experts, and a continuing effort to cast People's War as a viable concept under conditions of informatization.

Another concept apparently under continuous discussion is the term information superiority (IS). The book *The Theory of Military Information Superiority* demonstrated two things: that a single definition for IS has still not been developed; and that there

are definite plans underway for conducting both offensive and defensive actions on the cyber battlefield. The discussion of IS demonstrated that authors interpreted the term differently. Elements that stood out included the following:

- To achieve IS one needs to possess stronger information, acquisition, utilization, and control capabilities than the adversary;
- IS has two aspects, quantity and quality;
- IS is established in peacetime. It is unleashed just before war;
- IS's real significance lies in controlling the "time initiative";
- IS refers to a conflict between two parties, with one's exploitation capabilities stronger than the other's;
- IS as an equation is represented by the friendly side's information capabilities divided by the blue side's information capabilities;
- IS means having a greater degree of weapons informatization, a greater ability to acquire and process information, and a greater ability to attack and destroy an opponent than the abilities possessed by an adversary;
- IS is a higher level of superiority than force superiority.

Finally, the similarities and differences in the Chinese and Russian approaches to cyber issues were listed. Similarities include the following:

- Both countries are signatories to the Code of Conduct;
- Both countries worry about cyber's influence on the public and continue to support State-run television networks and other media to insure control of public opinion;
- Both countries are working on GPS systems, Beidou in China and Glonass in Russia;
- Both countries have begun a focused development of new concept weapons as a source of asymmetrical counter weapons, to include electromagnetic pulse, rail guns, nanotechnology development, and so on;
- Both countries rely heavily on Marxist thought.

Differences include:

- Russia is in a soft power protection mode while China is in both a soft power protection mode and also in a strong offensive projection mode at the present time.
- Overall, the Russian side does not seem to have as many clarifying cyber terms (water army, human flesh engine, etc.) as the Chinese.
- China has not developed an information concept to date for its military as the Russians have done with their "Conceptual View" document.

Conclusion

China's huge computer-focused population ensures that it will be a contender for cyber supremacy in the coming years, as quantity exhibits a quality all its own. It is clear that the activists and planners of Chinese information war intend to create a first class cyber apparatus. They are constructing a cyber organization and infrastructure to control digital processes; are educating a new breed of officer and serviceman with information-era activities; and are placing both infrastructure and education into a century old system of strategic thought that will adapt to these circumstances.

The three faces of the cyber dragon, peace activist, intelligence or reconnaissance activist, and attack planner, will continue to work in harmony toward achieving a goal of future cyber domination over any potential opponent. A May 2012 *Jiefangjun Bao* Online report is yet another example of how the PLA is solidifying this prognosis. Authors Li Yinnian and He Changqi wrote that future combat systems will implement combat operations that sabotage the net before an opponent can seek an opportunity to win[653] (reconnaissance of nets allow for the application of the stratagem of "win victory before the first battle"). The combat notion must be established that "whoever sabotages the net first wins and innovating methods of operations around sabotaging the net are an urgent thing to do."[654] The PLA must "directly take the network as the focus of sabotage," where key nodes and links must be destroyed with precision attack measures (attack planning). System sabotage also includes the application of means and methods to deceive, bewilder, and control a network control center in order to bring about soft kills[655] and achieve the goal of cognitive control (peace activist use of soft power). Western nations should remain wary of these three avenues of approach as they ponder future studies of Chinese cyber strategy.

653 Li Yinnian and He Changqi, "Whoever Sabotages the Net First Wins—Concept of Winning in Cyberspace Era," *Jiefangjun Bao* Online, 24 May 2012, p. 10.

654 Ibid.

655 Ibid.

APPENDIX ONE:
IW ARTICLES IN *CHINA MILITARY SCIENCE*:
2009-2011

The titles listed in English below are from the journal *China Military Science* and are representative of the IW content of this PLA journal. *Dragon Bytes* listed the IW articles in this journal from 1999-2003. *Decoding the Virtual Dragon* listed IW articles from 2004-2006. The *Dragon's Quantum Leap* covered these articles from 2007-2009. This section thus updates that list. The titles in this section are listed as they appeared in *China Military Science*, starting with the most current issue available and working backward to No. 1, 2010. As noted earlier, all PLA journals and newspapers continue to write extensively on the subject of informatization in China.

To continue a procedure initiated in *Dragon Bytes*, only those titles with "high-tech," "digitalization," "precision," "network," "system of systems" or "information" in the title are listed. Any Chinese discussion of US IO is also listed as are articles about psychological operations since they are an ingredient of Chinese IW.

Number 6, 2011

"A Study of Hu Jintao's Important Instructions on Enhancing Capabilities in Accomplishing Diversified Military Tasks with Winning Local Wars under the Informationized Conditions as the Core," Liu Yongming, Jin Zhenxing, pp. 1-9.

"Considerations on Systemic Warfighting Capabilities Based on Information Systems," Li Chunli, Pan Jinkuan, pp. 91-97.

Number 5, 2011

"Strategic Considerations on Informationization of Military Political Work," Dai Weimin, pp. 80-88.

Number 4, 2011

None

Number 3, 2011

"A Theoretical Exploration into the Soft Power in China's National Defense," Xiao Jingmin, pp. 131-138.

Number 2, 2011

"An Analysis of Fighting Styles in Informationized Warfare," Shi Daoxiang, Wang Junxue, Li Qu, et al., pp. 9-12.

"On Core Military Capabilities in the Information Age," Shen Genhua, pp. 44-52.

"From Two and Three-Dimensional Thinking to Networked Systemic Thinking—A Key Factor in Accelerating the Transformation of the Mode of Generating Warfighting Capabilities," Li Guangyu, pp. 110-112.

"An Analysis of the Concept and Mode of Battlefield Information Flow and Transfer in Network-Centric Warfare of the US Military," Yao Chunqing, Hao Dongbai, Liu Kue, et al., pp. 140-147.

Number 1, 2011

"Theme Forum: Theoretical Researches on Systems Operations Based on Information Systems" included these articles:

"An Explorative Study of the Laws in Developing Capabilities for Systems Operations Based on Information Systems," Wang Xiaoming, pp. 1-6.

"A Study of Basic Issues on Systems Operations Based on Information Systems," Geng Weidong, Zhu Xiaoning," pp. 7-12.

"A Technological Perspective on Capabilities for Systems Operations Based on Information Systems," Li Shouqi, pp 13-18.

"Thoughts on Building Military Force Structure Based on Information Systems," Lin Dong, pp. 19-24.

"A Tentative Study of the Information Enabled Mode of Formation of War-Fighting Capabilities," Dong Youxin, Cao Jiang, Liu Donghong, et al., pp. 25-33.

"A Study of Basic Issues on Systems Integrated Training Based on Information Systems," Zhang Jian, pp. 34-39.

"A Guidance for Mobilizing Capabilities for Systems Operations Based on Information Systems," Shang Zelian, Zong Xiangui, Huang Xiangliang, et al., pp. 40-44.

Additional articles in this issue:

"Reform of Command in Political Work during Wartime from the Perspective of Changes in Informationized Operational Mechanisms," Song Baohua, Li Jianhua, Liu Zhiguo, pp. 121-126.

Number 6, 2010

"PLA Informationization and the Development of a Space Military Force," Mu Zhiyong, Zhu Daobin, Liu Zhenbing, pp. 85-92.

Number 5, 2010

"Theme Forum: Theoretical Research on Systems Operations Based on Information Systems" included these articles

"Build a New Type of Operational Force Capability System Based on Information Systems," Zhang Hong, Yu Zhao, pp. 10-16.

"A Study of Information-System-Based Network Operations Theories," Li Daguang, Han Yufeng, pp. 17-23

"Thoughts on Raising Information-System-Based Maritime System of Systems Operations Capability," Jiang Lei, pp. 24-31.

"Information-System-Based System of Systems Operations Command Capability and a Study of its Applications," Li Yanbin, Zhang Ce, Wu Hongqi, pp. 32-41.

"Information-System-Based System of Systems Operations Adapt to the Requirements of Systems Operations Based on Information Systems and Promote the Reform and Innovation in Army Political Work," Research Center for Army Political Work of the AMS, pp. 42-46.

"A Study on Improving Core Logistical Support Capability in Information-System-Based System of Systems Operations," Gao Dongguang, Wang Youlin, pp. 47-51.

"On Training Modes of Information-System-Based System of Systems Operations Capability," Wang Shulin, Zhang Yingjie, Jia Chunjie, pp. 52-61.

"A Study of the Application of Nuclear, Biological, and Chemical Defense Forces Based on Information Systems," Wu Guoqing, Hu Xiaoping, Huang Yanwei, Lu Xin, pp. 62-66.

Additional articles in this issue:

"A Summary of Views at the Symposium on Systems Operational Capability Based on Information Systems," Shi Daoxiang, Xu Jianhua, Fu Qiang, pp. 150-156.

Number 4, 2010

"Theme Forum: Theoretical Research on Systems Operations Based on Information Systems" include four articles

"Preliminary Understanding of Information-System-Based System of Systems Operation Capabilities," Ren Liansheng, pp. 26-33.

"A Study of the Mechanism of Information-System-Based System of Systems Operations," Ping Zhiwei, Zeng Xiaoxiao, Zhang Xuehui, pp. 34-43.

"On the Composition and Basic Mode of Generating Information-System-Based System of Systems Operational Capabilities," Yan Zhensheng, Liu Haijiang, Feng Wei, pp. 44-50.

"Considerations for the Guidance of Information-System-Based System of Systems Operations," Luo Xiangde, pp. 51-58.

Additional articles in this issue:

"Dialectical Consideration on Operational Guidance under Information-ized Conditions," Yang Baoming, Zhao Changjun, Xu Jianhua, pp. 73-83.

"An Analysis of PLA's Image-Building from the Perspective of Military Soft Power," Tian Xiang, Chen Yongqiang, Ding Jun, pp. 116-124.

Number 3, 2010

None

Number 2, 2010

"On Main Operational Forms of Local Warfare under Informationized Conditions," Dong Xuezhen, Ren Desheng, pp. 15-23.

"On the Art of Controlling War Situations in Informationized Warfare," Zhang Yu, Liu Sihai, Xia Chengxiao, pp. 24-31.

"An Interpretation of Key Concepts on Joint Operations under Informationized Conditions," Geng Weidong, Zhu Xiaoning, pp. 32-40.

Number 1, 2010

"Experience, Lessons, and Theoretical Exploration of the Application of Network Science by the US Military," Zeng Xianzhao, pp. 127-132.

Number 6, 2009

"The Nature of Psychological Warfare: 'Spiritual Warfare' as Opposed to War of Flesh and Blood—A Philosophical Perspective on the Nature of Psychological Warfare," Cai Yongning, Wu Juncang, Zheng Dayin, and Fan Mingqiang, pp. 119-126.

Number 5, 2009

"On Relations between Military Soft Power and Comprehensive National Power and State's Soft Power," Long Fangcheng and Li Decai, pp. 120-129

"Study of Network Warfare in Terms of International Law," Zheng Guoliang and Zheng Ming, pp. 130-135.

Number 4, 2009

"Air Superiority in Local Wars under Informatized Conditions," Wu Wenjun and Tan Fuzhi, pp. 77-83.

"On Fire Warfare under Informatized Conditions," Li Yun, pp. 84-89, 97.

Number 3, 2009

"Analysis of New Changes in Principles of Information Warfare," Wang Hui and Geng Haijun, pp. 18-23.

"On the Nature and Categories and Forms of Information Operations," Dong Xuezhen and Tian Yuping, pp. 24-35.

"Considerations on Innovative Development of Military Armament Science under Informatized Conditions," Guo Shizhen, pp. 79-90.

"Fundamentals in Theories of PLA Informatization," Li Jing, pp. 100-105.

Number 2, 2009

"Transformation of Military Science Research Patterns under Informatized Conditions," Geng Weidong and Jiang Shaosan, pp. unknown at time of printing.

"Recent Development in the Study of the Idea of People's War under Informatized Conditions," Wang Wei and Yang Zhen, pp. unknown at time of printing.

Number 1, 2009

None

APPENDIX TWO:
GEOTHINKING LIKE THE CHINESE:
A POTENTIAL EXPLANATION OF CHINA'S GEOSTRATEGY

Introduction

Strategy formulators can only understand things and carry out innovative practical activities against the background of a specific social, historical, and cultural environment and tradition…understanding the adversary's ideological culture and strategic thinking method is as important as finding out the adversary's military deployment.[656]

—Li Jijun, Chinese strategy expert and former Deputy Commandant of the Academy of Military Sciences

China's number of perceived "national interests" and strategic orientations continue to grow. Internationally they can be found in new initiatives to develop the Panama Canal; in developing the cyber infrastructure or oil fields of Africa; in dominating the business environment of Singapore; in exploring more arms sales with Venezuela; or in the exploration of space, the new "high ground" (along with the cyber or information domain) in China's estimation. Closer to home, China's focus remains fixed on the geographic entities of the South China Sea, Taiwan, and contested parts of India. There are varying reasons for these interests, some internal (social stability), some external (new avenues for commerce or energy supplies), and some that are both (national security concerns).

The strategic thought process behind these geographical focal points is unlike those utilized in the US and other areas of the West, where the concept of ends, ways, and means dominates much of our understanding of strategy. China's strategic thought process is different. It is by design and history much more comprehensive and diverse. More importantly, underlying this evolved concept of strategy are three components or subthemes: *shi*, stratagems, and an objective-subjective thought process, all of which receive scant attention in the West in reference to "strategy." *Shi* refers to the attainment of a strategic advantage over an opponent; a stratagem is a Chinese historical proclivity designed to mislead an opponent's perception and thinking processes; and the objective-subjective thought process has two aspects. First, objective reality refers to material things. Second, subjective thought refers to the ability to manipulate objective reality. They are considered as a whole. It is postulated here that these components play an important role in helping China determine strategic targets and in manipulating historical, geographical, economical, military, and political issues in order to achieve strategic objectives.

This paper initially defines these components in more detail. The explanation

656 Li Jijun, "Military Strategic Thinking and Scientific Decision-Making," *China Military Science*, No. 1 2006, pp. 28-38.

is descriptive and meant to be thought-provoking. It is not proposed here that they represent a definitive solution to understanding Chinese geostrategy, but rather that they offer alternate methods through which to examine Chinese strategy (and better develop counters to confront China's strategic moves). In this sense the analysis follows Li Jijun's advice that "understanding the adversary's ideological culture and strategic thinking method is as important as finding out the adversary's military deployment." Both military and civilian journals are used in the analysis, while mostly military journals are used for defining strategy and its subcomponents.

After defining China's strategic components the paper then proceeds to look at China's concept of national interests (and their protection and advancement) and China's concept of the objective environment (instead of the "operational environment" descriptor of the US military). Finally, the paper uses the strategic definitions and focus on national interests and objective reality to better understand some potential Chinese strategic guidance. China's external and internal strategic resource strategy is based on its needs and capabilities. Two truncated case studies are considered: the nation's external need for oil (focusing on oil interests in Africa and its transport through the South China Sea) and China's internal abundant supply of rare-earth elements. The geostrategies associated with these external and internal strategic resources are quite different. The paper concludes with an assessment of China's needs and capabilities versus the resource strategy it has developed. In short, the conclusion is an assessment of China's geostrategic plan.

This analysis doesn't portend to look at Chinese strategic policy, decision-making, military planning, and so on through "blue" glasses, i.e., templating these processes via US patterns. Rather, this is an attempt to get into the Chinese mind-set. The emphasis is on presenting these processes through the prism of Chinese thought as closely as possible from Chinese, not US, open-source materials. For that reason, more time is spent on defining terms for the reader. Finally, several terms are highlighted in **bold** throughout the paper so that readers are able to recognize and find new authors and dates quickly and chronologically as well as follow the thought processes associated with geostrategic issues.

Defining Geostrategy

Chinese senior captain **Xu Qi**, a deputy director of the Strategic Research Office of the Navy's Military Academic Research Institute at the time his article appeared in **2004** in *China Military Science*, offered a definition and description of geostrategy. He wrote that geostrategy is "the state's strategy for seeking and safeguarding national interests in the realm of foreign relations."[657] Further he noted that geostrategy makes "use of geopolitical relations and the rules governing such relations in the international realm" and takes "state-to-state geopolitical relations as the object of research, such geopolitical elements as the geographical position, the comprehensive national

657 Xu Qi, "Sea Geostrategy and the Development of the Chinese Navy in the Early 21st Century," *China Military Science*, No. 4 2004, pp. 75-81.

strength, and the distance in space…"[658] "Distance in space" issues refers to the fact that interests decrease when space increases while the shorter the space distance, the more serious the threat to national interests. Geopolitical factors and the geographical factor are the two basic elements of geostrategy in Xu's opinion. The former is changeable while the latter, due to environment and position, is more stable.

After the early exploration period of the 15th century China closed off its borders to the outside world. Survival became rooted in control of land space and not the sea. As a result geostrategic thought ignored the sea for years. In many ways this was understandable since there were no sea powers that threatened China. For the mainland, the seas along its extensive border served as a shield and guardian of the mainland. Today, there is a historic opportunity for China to develop its maritime geostrategy due to the extensive change in the international situation after 9/11 focusing on integration and to new maritime geo-security threats to China's coastal areas.[659] Xu notes that "for China, a country with the greatest population in the world and with relatively scarce resources, the seas provide the most important strategic space for the country's sustainable development and also represent the strategic substitute zone of its land resources."[660] The seas will promote China's future development and the Navy must develop its capabilities to defend the nation's sea territory. With regard to defending national interests in the information-age, Xu wrote:

> The use of informationized advanced weapons, space weapons, and new concept weapons will make it possible to launch multi-dimensional precision attacks from a broad scope stretching from the first island chain to the high seas, thus threatening the important political, economic, and military targets in the deep strategic rear areas. As threats to maritime security will come from the distant opens seas, the Navy is required to broaden its vision to the open seas, develop its attack force for fighting in exterior lines, and set up necessary shields for the long-term development of national interests.[661]

Xu adds that marine space, air space, and outer space, also known as grand strategic or public space, belongs to no country. International waters, according to his calculations, occupy 64 percent of the total oceanic space on earth. China aims to take part in the management and protection of the resources therein. Interestingly, he states that China "has extensive national interests in the 'international waters' and the 'international voyage straits.'" This is based on transportation routes and the fact that China is the fifth largest investor in the international seafloor zone. National interests will extend to all parts of the world's marine space where China economy is involved. This requires naval safeguards of such interests.[662]

658 Ibid.
659 Ibid.
660 Ibid.
661 Ibid.
662 Ibid.

China's geographic location is in a part of the world where the geostrategic interests of many of the world's big powers collide. Each nation has a different method for solving its interests and the path it takes is reflected in its national security strategy. While not defining geostrategy directly, one authoritative Chinese military reference book states that a geostrategic relationship between states means "strategic relations relevant to the interests between related states formed on the basis of national geography and geocircumstances, such as geopolitical relationships, geomilitary relationships, and so on. These relationships play a basic role in national security and development and are important elements to influence and restrict war and strategy."[663] Two classes of elements make up a geostrategic relationship: natural geographic elements (a state's geographic position, size and shape of its territory, natural resources, capital, national frontiers, and boundaries, etc.); and a state's comprehensive power of economy, science, and technology; culture and the military; the organic structure and distribution of manpower resources; the structure of nationalities, religions, and social forces; a state's position of its role in the international community; and the characteristics of its foreign policy, among other issues.[664]

Natural resources (in the case of this paper, strategic resources) are a focal point of the analysis. These resources are the **objective** conditions on which the existence and development of a state depend. They include regenerative resources (land, water, biology, etc.) and non-regenerative resources (mineral resources, fuel, etc.).[665] This paper focuses on the latter area.

Defining Strategy

Strategy remains an area of intense focus, most likely due to its long historical roots as a Chinese tradition. Today, the topic is often discussed in military journals. For example, in the 2009-2010 issues of the journal *China Military Science*, an important People's Liberation Army (PLA) publication, there were twenty-two articles focused on strategic concepts, a concentrated focus unlikely to be found in US journals (see list at end of Appendix Two).

The best single work on Chinese strategy, in this author's opinion, is the **2001** Chinese book *The Science of Military Strategy*. It is an excellent treatise on the Chinese concept of strategy and all of its inherent elements. Authors **Peng Guangqian** and **Yao Youzhi**, long considered experts in their field, defined military strategy in the following manner:

Strategy in China's new period takes national comprehensive power as its

663 Peng Guanqian and Yao Youzhi, *The Science of Military Strategy*, Military Science Publishing House (English Edition), p. 62. The English translation of the book, published by the Chinese, appeared in 2005.

664 Ibid.

665 Ibid., p. 64.

> foundation, the thought of active defense as its guidance, and winning local war under high-tech conditions as its basic point to construct and exercise military strength; it carries out the overall and whole-course operation and guidance of war preparations and war for the purpose of protecting national sovereignty and security.[666]

Absent from this official definition is any mention of the **objective-subjective** thought process, stratagems, and *shi*. It includes a holistic view of "China's new period" and stresses two of China's core interests: sovereignty and security. Another work, the *Chinese Military Encyclopedia*, also ignores the subcomponents of strategy, defining it as

> The general plans for planning and directing war situations as a whole. That is, based on analysis and assessment of the international situation and the various political, military, economic, scientific, technological, and geographical factors of the two hostile parties, scientifically calculating the occurrence of war and its development, formulating strategic policies, strategic principles, and strategic plans, planning war preparations, and all of the principles and methods followed while directing the implementation of war.

This definition discusses planning and directing a war effort based on an assessment of the situation and an analysis of various factors. It concludes by stating that one must calculate war's probability and formulate the principles used to direct war's implementation.

These two definitions are radically different from one another. The first appears to be more contemporary and focuses on comprehensive national power and war preparations under information conditions. The second definition focuses on planning and directing war from strategy's more historical vantage point. However, if neither mentions the **objective-subjective, stratagem**, and ***shi*** processes, then why are they the focal points of this paper? What do they have to do with strategy? The answer is that the **objective-subjective** thought process and **stratagems** suggest the HOW behind comprehensive national power and the planning process, while attaining ***shi*** accomplishes one of the actual primary goals of strategy. All three processes are imbedded in Chinese planning implicitly much as empirical thinking is imbedded in the thought processes of some Western countries.

A Quick Overview of the Process

From an outsider's perspective there appears to be a few steps involved in developing strategic concepts and making decisions. The process starts with a comprehensive

666 Ibid., p. 12.

overview of **objective** reality. The threats, geographical conditions (resources, passages, borders, etc.), needs and excesses, levels of spending on defense and research in a nation, and so on are the elements of **objective** reality, the concrete things or material stuff of the contemporary environment. From **objective** reality, **core interests** are determined, as well as the major and general interests of the nation.

The game of strategy begins to evolve as nations decide which interests become requirements for the nation's survival. It follows that the ways to "get what you want" are manifested as strategic guidance (**stratagems**). The goal is to achieve a strategic advantage (***shi***) of some kind that can be exploited now or in the future. The process involved with gaining a strategic advantage is sometimes referred to as the **subjective** thought process. It involves finding ways to manipulate **objective** reality to one's benefit. The **subjective** thought process can utilize **stratagems** in the search for attaining strategic advantage or ***shi***.

Conditions are changing constantly in the information age. These changes may be the result of fast scientific and technological changes, issues of globalization, or pure web influence. **Objective** reality, **subjective** methods of manipulation, and the utilization of change and new knowledge are the major elements involved in determining a nation's risk-taking calculus. Risks may be taken at crucial points if the elements indicate success. Or risks may be taken that allow for the use of certainty or even uncertainty (for example, when uncertainty is used as a component of deterrence theory). The application of these thought processes results in change through strategic guidance.

The Objective-Subjective Thought Process

*Military strategy consists of planning and guidance for the situation of military struggles as a whole; it means taking an **objective** approach with **subjective** matters.*[667]

Just what is meant by the objective-subjective thought process? The Chinese *Xinhua Cidian* (*Xinhua Dictionary*) states the following:

> **Subjective refers to a person's thinking or understanding. Objective refers to the material world existing outside of a person's consciousness**. The relationship between subjective and objective is a dialectical unity. Objective does not rely on subjective and exists independently, it is the source of subjective, it determines subjective; subjective reflects objective, and actively reacts with objective, under certain conditions it determines the effect of objective. The objective world is constantly developing and changing, and a person's understanding must also accordingly develop and change. There are frequent contradictions between subjective and objective. Only through practicing constantly to overcome the contradictions between subjective and objective does subjective understanding accord with objective reality, and

667 Fan Zhen Jiang and Ma Bao An, *On Military Strategy*, National Defense University Book Series, 2007, p. 59.

> only then can the world be effectively changed. Idealism and mechanical materialism, and opportunism and adventurism, are all divided by subjective and objective and are characterized by the separation of understanding and practice.[668]

Objective thought refers to the reality one faces, the concrete factors that are to be considered. These include issues such as the level of science and technology in a nation, the nation's portion of the budget spent on defense, the location of its troops, and so on. **Subjective** thought refers to a policy makers' or commanders' ability to influence or manipulate objective factors for their benefit.

The issue of objective-subjective thinking dots **Peng** and **Yao's** work. The topic first appears in the section on the laws of strategic thinking. In this section of the book, the authors list five models of strategy. The very first model states that "strategic thinking can be divided into an **objective** strategic thinking model and a **subjective** strategic thinking model according to the character of thinking."[669] The second model notes that "strategic thinking can be divided into a closed strategic thinking model and an open strategic thinking model according to the degree of openness of the thinking."[670] The third model states "strategic thinking can be divided into a **stratagem** type strategic thinking model and a force type strategic thinking model according to different application of strength by strategic subject."[671] The fourth model notes that "strategic thinking can be divided into conservative strategic thinking and creative strategic thinking according to the attitude of the thinking toward experience and tradition."[672] The fifth and final model states that "strategic thinking can be divided into unitary strategic thinking and systematic strategic thinking according to the quality and scope of the thinking subjects' knowledge."[673] The recent Chinese focus on system of systems methodology over the past year and a half indicates that the fifth model has received an elevated status (see the author's forthcoming "Is China Channeling Admiral Owens?" for a comprehensive overview of the system of systems discussion).

When discussing war strength, war potential, and the means to win war and secure military objectives, Peng and Yao reference a famous historical statement on the **objective-subjective** thought process. Mao, they note, stated that war is a contest in **subjective** ability between the commanders of the opposing armies in their struggle for superiority and for the initiative on the basis of material (**objective**) conditions such as military forces and financial resources.[674] When making strategic decisions, the HOW of strategy, Peng and Yao write that "All correct strategic decisions are products of the conformation of **subjective** knowledge to **objective** reality. Strategic decision, as a thinking and cognitive activity, is not made without foundation nor is it innate in the

668 *Xinhua Cidian* (*Xinhua Dictionary*), 1985, p. 1106.
669 Peng and Yao, p. 134.
670 Ibid.
671 Ibid., p. 135.
672 Ibid., p. 137.
673 Ibid., p. 138.
674 Ibid., p. 57.

mind of the strategic conductor but is the reflection of the laws of the movement of war and the embodiment of laws of strategic thinking."[675]

Decision-making consists of judgments about the strategic situation, a decision on the strategy to accept (a decision on strategic guidance), and a formulation of strategic plans from this.[676] The authors note that the artistic character of strategic guidance lies in its wise application of **stratagems**. **Stratagems** (discussed more deeply in the next section) and **subjectivity** are thus closely related.

Subjective ability (the contest between opposing commanders) refers to the use of **stratagems** by commanders to gain an advantage and superiority over an opponent. **Stratagems** are based on trickery or diverting an adversary's attention to his detriment. **Stratagems** are one of the six characteristics of strategy, according to Peng and Yao. They note that

> Strategic guidance means a competition of strategic wisdom and **stratagems** on the basis of certain physical strength. The artistic character of strategic guidance lies in its wise **stratagems**. Accordingly in strategic contest a strategic conductor's **subjective** initiatives are highly expressed in his resourcefulness and decisiveness, circumspection and far-sightedness, flexibility and responsiveness, and surprise moves to defeat the enemy. Outstanding levels of **stratagem** can ignite an extraordinary energy from the national strength available and turn the passive to the active and transfer inferiority to superiority as to secure the objective of winning by a few and winning superiority by using inferiority.[677]

Beside stratagems, other characteristics of strategy are practice, politics, comprehensiveness, antagonism, and prediction.

The strategic material or **objective** base of China's military strategy is "comprehensive national power." **Objective** reality is based on actual military strength and power while **subjectivity** implies the ability to manipulate reality (via **stratagems**, wisdom, and resourcefulness) to gain superiority of some type (psychological, situational, actual, etc.) and thus the initiative.

Peng and Yao also provided an overall view of strategy from a Marxist viewpoint:

> The **objective** physical conditions of war determine the laws of war as well as the guiding laws of war. Although strategy manifests itself in a war conductor's activities of **subjective** guidance, it is by no means the war conductors' personal extemporaneous elaboration. Instead it is based on given **objective** physical conditions and restricted by a certain social mode of production and certain social conditions of history. Therefore, it is an important task for studies of the science of strategy to correctly analyze the **objective** elements

675 Ibid., p. 174.
676 Ibid.
677 Ibid., p. 28.

having a bearing on war strategy and reveal their inherent connections with war strategy.[678]

Wang Pufeng wrote in **2004** on the topic of strategic thinking.[679] He stated that thinking and ideas are not the same thing. Thinking "refers to the process of using a certain method to carry out a reasonable understanding. Ideas are the results of the thinking process." Thinking places more stress on adhering to principles and methods and not on results. As the **objective** world constantly changes, so also does the strategic situation. Innovative approaches are required to handle unexpected changes. Innovative thinking, according to Wang, is

> The flashpoint of strategic thinking; it is the ladder for successful strategists; it is the concrete embodiment of the knowledge and talent of strategists; it is the light of the art of strategic thinking. It may be said that there are no strategists who have no innovative thinking.[680]

Wang then asks "Does the obliquity in strategic developments have innovative strategic thinking as its **subjective** driving force?" It appears the answer to that question is "yes." The main body of strategic thinking is composed of expert knowledge of the situation, knowledge gained from experience and study, and outstanding ability (wisdom and knowledge) and sagacity (strategic planning and management). The latter two are the essential elements of strategic thinking in Wang's view.[681]

Zhang Shiping, writing in **2007** in the journal *China Military Science* about the nature and characteristics of strategy, noted that major issues in politics, the economy, culture, and society are called policy, while major issues in military fields are called strategy. He listed factors that could be considered as **objective** to include "armed forces building, defense works, manufacturing and storing military equipment and military goods, war mobilizations, determining basic operational orientation, differentiating theaters of operations, and formulating combat policies and principles of combat guidance."[682]

Zhang listed what he considered as the "**objective** formal characteristics" of strategy:

---

678 Peng and Yao, p. 39.

679 Wang Pufeng, "On Strategic Thinking," *China Military Science*, No. 3, 2004, pp. 86-91. When referring to strategy's nature, Wang listed a host of adjectives: scientific, comprehensive, macroscopic, social, multi-dimensional, confrontational, astute and resourceful, decision-making, stable, definite, flexible, predictive, forward looking, technical, innovative, and so on. He defined strategic thinking as "the overlapping discipline of military science and the science of thinking; it is the fusion of strategics and the science of thinking." Strategy is macroscopic, calculated, key-point oriented, innovative, and dialectical (with the latter element undergoing changes as war develops). It is a contest between the guiding thoughts of adversarial and friendly elements.

680 Ibid.

681 Ibid.

682 Zhang Shiping, "Connotations, Nature, and Characteristics of Strategy," *China Military Science*, No. 6 2007, pp. 53-59.

- Strategy is a historical category
- Strategy has a hierarchical nature. Major categories are international, grand, national, national security, and national military strategy. Minor ones are combat, military service, theater of operations strategy, and so on. National strategy includes war preparations and war implementation, categories that national security organizations consider.
- Strategy's substance changes during different periods of time and at different levels. Today, national strategy and military strategy are the central considerations.683

After listing these objective issues, Zhang discussed **cognitive** (subjective) methods. He wrote that "policies, strategic guidelines, and **stratagem** are closely related to strategy."[684] He states that "strategy is a matter of the objectives, general guidelines, policies, and principles related to national security, war preparations, and war implementation; and a **stratagem** is a scheme or tactic used in the methods and measures for strategic planning and strategic practices." Strategic guidelines, he adds, can include concepts such as "lure the enemy in deep" or "active defense."[685]

A **2007** book, *On Military Strategy*, explained the Chinese concept of strategy.[686] The book describes the military strategy concept and its components. Included in the explanation were characteristics, missions, the **objective** environment, planning, management, war direction and control, guiding ideology, and war mobilization. The book provides several hints as to how to conduct strategic analysis as well.

The authors write that military strategy consists of three elements: strategic objectives and strategic missions, strategic policy; and strategic measures. Strategic objectives are methods in pursuit of political goals while strategic missions are problems that must be resolved through military struggles. Objectives and missions change according to different stages in history. Strategic policy provides the basic approach for fulfilling the missions and realizing the objectives. It is a scientifically formulated strategic policy developed by the Central Military Commission. Strategic measures represent the general term for military force and the methods for achieving missions and objectives. They are the methods for **subjectively** guiding and unleashing the material force. **Objective** realities are enhanced through relevance, flexibility, and suitability.[687]

China's renewed interest in military strategy occurred after the 1980s. It resulted in a three-tiered system of national strategy, national military strategy, and the strategy of the services, theaters of operation, and logistics. The authors note that **objective** possibilities and **subjective** efforts are interconnected and blended together, giving

683 Ibid.
684 Ibid.
685 Ibid.
686 Fan Zheng Jiang and Ma Bao An, *The Theory of Military Strategy*, Beijing National Defense University Publishing House, 2007.
687 Ibid., pp. 8-13.

military strategy a high degree of flexibility and diversity.[688] Military strategy has a political nature that determines its missions and tasks, an epochal nature in that these missions and tasks can change over time, and a guiding nature that selects the appropriate path, scale, and speed of development most beneficial to realizing national security interests of China.[689]

The issue of resourcefulness is of prime importance. Peng and Yao listed it as a sub-element of **stratagems**. The actual implementation of military strategy is expressed through choices in the use of opportunities, forms, and methods. This requires "strategic directors" to unleash **subjective** guidance, using strategy according to the situation and working to exploit adversarial traits. Successful strategies require resourceful thought. This requires "agile ingenuity" and methods such as using different countermeasures to deal with different circumstances or using a variety of resources and plans to deal with complicated situations. Resourcefulness makes up for shortcomings in military strength and the technological levels of weapons and equipment.[690] Further, strategic planning is witnessing a combination of traditional resourcefulness and modern high-technology measures, making strategy more flexible, rich, and clever.[691]

Finally, in yet another example of the use of the **objective-subjective** thought process, author Senior Colonel **Luo Xiangde** from the Nanjing Army Command Academy wrote in **2010** that the strategic system of systems thinking for China is "a strategic thinking activity in which **subjective** ideas are manifested through **objective** realities."[692] Thus, the concept is used quite often in military affairs when discussing strategy from a variety of perspectives.

Stratagems

When US planners gather to make decisions for an upcoming operation, they generate courses of action (COA). A commander then examines his options and decides which course of action provides the best chance for success. Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*, defines a course of action as

> Any sequence of activities that an individual or unit may follow. 2. A possible plan open to an individual or commander that would accomplish, or is related to the accomplishment of the mission. 3. The scheme adopted to accomplish a job or mission. 4. A line of conduct in an engagement. 5. A product of the Joint Operation Planning and Execution System concept development phase and the course-of-action determination steps of the joint operation planning process.[693]

688 Ibid., p. 27.

689 Ibid., pp. 43-45.

690 Ibid., p. 19.

691 Ibid., p. 20.

692 Luo Xiangde, "Considerations on Guidance for Information-System-Based System of Systems Operations," *China Military Science*, No. 4 2010, pp. 51-58.

693 Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*,

When Chinese planners gather to make decisions, they consider the **objective** factors before them and then generate potential **stratagems** for use by commanders instead of COAs. A **stratagem** is a concept designed to mislead an enemy's perception, thinking, and emotional processes. Its function is to fool an enemy force whereas a COA is designed to take advantage of a situation or, as the definition states, it is a scheme adopted to accomplish a mission. These definitions have been used for years but they differ in intent. The concept of manipulation appears to be inbred in a stratagem but not as clearly in a COA. However, Desert Storm COAs used the manipulation of reality (a fake marine landing before the "left hook") so manipulation is not a lost art in the US.

Today, one factor that COAs and **stratagems** share is a reliance on information technology (IT) components. Due to rapid advances in science and technology, the Chinese see IT as a valuable asset and feel that "the contents of the **stratagem** are continuously changing and renewing; the methods of **stratagem** are becoming more comprehensive; the space encompassed by the **stratagem** is multi-directional; and the technological content in **stratagem** methods are unique."[694] **Stratagems** thus remain an effective way of planning for engagements with an opponent and manipulating an opponent's reactions. For the US armed forces, IT offers ways to better integrate and coordinate COAs.

To win with **stratagem** in the information age the PLA believes that a strategist must link technology, strength, and **stratagem** to control victory. A good strategist is a good thinker who is innovative, creative, and flexible in his use of **stratagems**. A good **stratagem** performs a host of cognitive tricks, to include deceiving, controlling, inducing, arousing, creating, innovating, or manipulating another person or an entire staff.

Zhang Xing Ye and **Zhang Zhan Li**, the editors of the **2002** book *Campaign Stratagems* (a book published by China's National Defense University Printing House), note that "the side being in a strategically superior position, planning first and fighting later, winning through strategy, is able to fully promote high-tech superiority…"[695] A human's control over high-tech weapons and his or her ability to integrate weapons with **stratagems** makes one maximally effective.[696] The editors further state that in Chinese, *moulue* is **stratagem**, trick, and/or tactic. The concept is adaptable to decision-making, **subjective** initiative, and deception, and it is applicable to politics, the economy, international affairs, and military affairs.

Li Qi writes in the introduction to *Campaign Stratagems* that a campaign **stratagem** is when "the commanding officer, on the basis of certain strength, fully performs his **subjective** initiative, and manipulates and drives the enemy in the confrontation of

12 April 2001 (as amended through 19 August, 2009 at the time of this writing). The Internet version can be found at http://www.dtic.mil/doctrine/dod_dictionary/index.html.

694 Zhang Xing Ye and Zhang Zhan Li, *Campaign Stratagems*, National Defense University, 2002, p. 249.

695 Ibid., pp. 4-5.

696 Ibid., p. 5.

intelligence, so as to create a situation that is favorable to his own troops but unfavorable to the enemy."[697] The transformation from static strength to operational efficiency requires the exploitation of friendly campaign strength, enemy campaign strength, and the campaign environment. This analysis is commonly referred to as uncovering *shi,* the sum of all the factors that impact on the performance of the respective operational efficiency of two sides in a general confrontational situation.[698] *Shi* is discussed in more detail in the next section.

A main element of campaign **stratagem** is the battle of wits. With action verbs such as manipulate, deceive, trick, and control, this is understandable. Editors Zhang and Zhang list three features of the battle. First is the competition of contradictory interests between two sides. Second is the manner in which decision-makers interact and attempt to influence one another. Knowing the decision-making process of one's opponent allows for the manipulation of that process. Third is the commander's personality and how he or she reacts under pressure in an uncertain environment. A study of hobbies, weaknesses, and flaws is "the best breach point for **stratagems**."[699] This implies that the Chinese conduct intense data-gathering on the personalities and interests of foreign commanders and leaders. For this paper, however, it is China's use of the stratagem battle of "competition of contradictory interests" that appears to be the most often noted by Chinese specialists.

There are three campaign **stratagem** methods. The first method is to "break up and unify," changing the balance of static strengths of both sides in terms of time and space. The second method is to use special and regular forces, applying general concepts in irregular ways. The third method is to use deception and real actions (alternating between them). Integrating these three methods can improve chances of success. The editors periodically mention these three methods throughout the text. When applying these methods, creativity and flexibility become the soul of a campaign **stratagem's** "battle of wits," since **stratagems** are the primary means for the creation of a situation.[700]

Simultaneously, the weaknesses and limitations of an enemy's high-tech equipment must be exploited.[701] The editors believe that differences exist among Chinese and foreign stratagem experts due to **objective** conditions, each nation's operational environment, and various cultural and military heritages. Under various conditions the concept of risk, for example, would be treated differently. Zhang and Zhang note that the PLA stresses being active and steady, pursuing certain victory, engaging in prudent early engagement (cyber reconnaissance?), encouraging reasonable risk-taking, and avoiding unfavorable decisive battles. In the opinion of the editors, Western armies use common sense as the primary component of their **stratagem** thought process, along with systems theory, information theory, control theory, images, intuitional thinking,

697 Li Qi, "Introduction to Campaign Stratagems," in Zhang Xing Ye and Zhang Zhan Li, *Campaign Stratagems*, National Defense University, 2002, p. 9.

698 Ibid., p. 11.

699 Ibid., pp. 12-14.

700 Ibid., pp. 14-15.

701 Ibid., pp. 44-46.

associative thinking, and psychology and behavioral science.[702]

Li Qi believes that the development of technology has opened up more avenues for the use of campaign **stratagems**.[703] Since the entire strategic depth is now open for exploitation, this creates more flexibility in target selection and the employment of **stratagems**. Engagement relationships are more complex due to the uncertain mix of symmetrical and asymmetrical operations.[704]

Li Qi writes that an understanding of "disposition" is crucial to **stratagem** application. This is similar to the concept of *shi* mentioned earlier. By disposition he is referring to force composition, battlefield environment, and campaign engagement methods. The concept of a force/superiority also has changed from concentrating forces such as troops and weapons to concentrating capabilities based on issues such as information mobility and long-range firepower. Capability superiority consists of the "mobile dispersal of entities (forces and weapons) and mobile concentration of capabilities." As an example Li used the Kosovo conflict where forces were dispersed all over Europe, the US, and space, yet operational capabilities were focused on an area to form theater superiority in what the US termed "global force integration." Long-range firepower and information mobility do not require the time or the infrastructure that ground troops require to concentrate assets on an area. It is also important to match a campaign **stratagem** with the overall political, economic, and diplomatic situation. Only when the stratagem matches the strategic situation can an enemy be convinced of an action.[705]

One section of *Campaign Stratagems* (perhaps the most important) is HOW to manipulate enemy commanders. The section opens by stating that not only high technologies, but also control theory, information theory, psychological theory, organization and behavioral theories, and the methodology of systems engineering science are required to guide a campaign **stratagem's** planning and execution. This includes rationally selecting campaign objectives and, most important of all, deductively devising **stratagem** information to control the "intelligence-judgment-decision" process of the enemy.[706]

To deductively devise **stratagem** information requires the meticulous preparation of special information. An information developer's application of a **stratagem** requires the creation, transmission, receipt, and processing of information as the developer intends. **Stratagem** information is based on the development of specific information for different control targets. Some control targets require three things: supporting information to affirm the correctness of an enemy's judgment; interfering information of an independent or contradictory nature; and the blocking of key information concerning friendly intentions. One should alter enemy commanders' original judgments. They must be fed negative information, supporting information, and

702 Ibid., pp. 46-47.

703 Li Qi, "Campaign Stratagem Application under High-Tech Conditions," in Zhang Xing Ye and Zhang Zhan Li, *Campaign Stratagems*, National Defense University, 2002, pp. 215-217.

704 Ibid.

705 Ibid., p. 228.

706 Ibid., pp. 239-240.

interfering information, and key information must be blocked.[707]

The developer of a stratagem must do everything possible to control the enemy's method of intelligence analysis and processing. This will put the stratagem developer in sync with the enemy's "intelligence-judgment-decision" process and induce the enemy to make decisions as one would expect him to do. The stratagem must consider the following points:

- Take into consideration an enemy's belief system, formed from knowledge structures, **subjective** leanings, method of thinking, and personality to meet concerns and needs and influence judgments.
- Take into account the enemy's decision-making organizational mechanisms. Anticipate distortions and insert redundancy of key information. Influence the basic characteristics of key individuals and links such as the intelligence processing procedures of the enemy.
- Take into account when sending out the first batch of **stratagem** information that it should be highly seductive and influential, followed by supporting information.
- Take into account political, superior/boss, and environmental pressures and their impact on decision-making.[708]

Transmission channels must be carefully controlled. Those channels that China controls completely, partially, or not at all are called white, gray, and black respectively. If black channels uncover friendly **stratagems**, then the **stratagems** can be used against friendly forces. This is the worst of outcomes, to fall into a counter-**stratagem** trap. The use of white channels that the enemy considers as reliable is the best for transmitting information. Further,

> We [China] must pay a lot of attention to the cultivation and development of reliable channels during peacetime so as to develop enemy trust in these channels and to transmit **stratagem** information during war time. Under high-tech conditions, a strong enemy tends to highly trust, and heavily rely on, high-tech intelligence reconnaissance means. Therefore we must pay close attention to the characteristics of the enemy's high-tech reconnaissance means and study effective deceptive measures.[709]

Invariably, Li adds, some **stratagem** information will be distorted or lost due to an inability to properly predict certain **subjective** or **objective** responses. As a result multiple channels must always be utilized. In addition, feedback channels must be established to monitor the success or failure of the **stratagem** and to avoid having a counter-**stratagem** developed by an enemy.

707 Ibid., p. 240.
708 Ibid., p. 242.
709 Ibid., p. 245.

Stratagems use the scientific way of thinking, which is a way "to analyze, design, research, manage, and control such a complicated system and provide the most optimized ways and methods."[710] It is first necessary to defeat an enemy by thinking and only later by action.[711] Simultaneously, what is termed "psychological position exchange" must be accomplished. This means making a parallel comparison with the opponent's thought processes in order to imagine what he would do and think, that is, to put oneself in one's opponent's shoes.[712]

In **2010 Xue Guoan** wrote on the characteristics of China's traditional strategic thought.[713] He appeared to focus more on cognitive aspects, to include soft power. Xue is an authoritative figure. He is the Deputy Director of the Department of Strategic Studies at National Defense University (NDU). The abstract that precedes his article notes the following:

> This thinking embodies the following distinctive characteristics: overall integrity, long-term **stratagem**, the combination of military and non-military strategies, equal importance attached to **stratagem** and real strength, priority to soft tactics, and the principle of gaining mastery by striking only after the enemy has struck…on the other hand, however, this thinking has such shortcomings and deficiencies as over-emphasis on classics, little attention to innovation, over-emphasis to principles but overlooking the role of armament and ignorance of the importance of maritime power.[714]

Xue notes that even in ancient China, consideration was given to the overall situation, since Sun Tzu used five factors (the way, heaven, earth, command, and rules and regulations) when considering warfare. "The way" refers to political manipulation, a method that allows people to "think in line with their sovereign." When considering the overall plan for war, it is necessary to take in the overall situation and use **stratagems** wisely in exploiting circumstances to one's advantage.[715]

Xue chides Western strategists for their tendency to embrace power, only resorting to **stratagems** as a last resort. The Chinese, on the other hand, as an agricultural society, embrace the natural environment and geographical factors. Descriptions of how stratagems are devised are as important as details of battles in historical works, he notes. Xue states that devising **stratagems** at the strategic level is a focus of Chinese practice. There is emphasis on how **stratagem** can coordinate the overall situation, enabling limited military power to generate "immeasurable efficacy." Another important aspects is to attach equal importance to stratagem and actual strength. Sun Tzu advocated winning by thwarting an adversary's strategy and then by disrupting his alliances.

710 Ibid., p. 263.

711 Ibid., pp. 263-264.

712 Ibid., p. 265.

713 Xue Guoan, "Characteristics of China's Traditional Strategic Thought," *China Military Science*, No. 3 2010, pp. 116-122.

714 Ibid.

715 Ibid.

By covertly reversing a power balance, one becomes stronger than one's adversary. Controlling one's use of power is thus paramount to success in soft tactics.

Using soft military power is reliant on building up one's latent military power and exhausting an adversary's overt power. Xue states that the key to using the strategy of soft military force is to apply "perfect stratagems to weaken one's adversary and maintain a low profile in developing one's national strength." Such a strategy is enhanced by a protracted war in which one strikes when the opportunity arises. One is reminded of Muhammad Ali's rope-a-dope tactic of waiting until his opponent exhausted himself by pounding away at Ali's covered up body. China advocates the same concept, switching to the offensive only after one's opponent has exhausted his power. However, Xue concludes with this advice: when a favorable opportunity for battle emerges, China must not stick to its moral concept of not firing first. Rather, China should use the opportunity to defeat an adversary in one move. Soft military power is equivalent to the strategy of active defense.

Modern warfare techniques showed that was not the case. A weakness was the overreliance on land power at the expense of sea power. Today, China is focusing much more attention on the latter. It is a key element of the country's geostrategy.

According to Zhang and Zhang, the PLA is developing institutions to prepare and monitor the use of **stratagems**. The PLA actively studies the analytical processes of foreign militaries to apply the proper **stratagem** techniques against them. Stratagem techniques enable the PLA to create a situation that is favorable to them. They are preparing for future "battles of wits" now in peacetime.

It is important that US national security personnel understand that these military capabilities can be applied to political, economic, and other fields of study. There may well be Chinese institutes in existence now that are involved in the study of campaign stratagems to manipulate US financial flows or to create other disruptive situations. The US and its allies must prepare now for such eventualities.

Shi

Different Chinese and English speaking authors have translated ***shi*** as energy, power, momentum, and strategic advantage, among other translations. Why should this concept be of any concern? Noted Western Sinologist Roger Ames has called the concept of ***shi*** "the key and defining idea in Sun-Tzu: *The Art of Warfare*." Ames translates the term as "strategic advantage." He notes that ***shi*** "is a level of discourse through which one actively determines and cultivates the leverage and influence of one's particular place."[716] The popular Western Sinologist Ralph Sawyer defines this type of ***shi*** as the "strategic configuration of power."[717] ***Shi*** is the title of Chapter Five of Sun Tzu's *The Art of Warfare*.

The examination of ***shi*** that follows is based on different linguists' translations of the concept in *The Art of War*, on the views of experts on the topic, and on definitions from dictionaries or philosophical compendiums. The examination allows one to

716 *The Book of War*, The Modern Library, New York, 2000, p. 50.

717 Ralph D. Sawyer, *The Art of War*, Fall River Press, 1994, pp. 143-147.

consider several linguistic variants of the term. The concept is also examined from the contemporary context of what might be expected from the "strategic configuration of electrons" or from one of the other definitions of ***shi***.

Shi is a Chinese term that has eluded a precise Western definition. It is a concept familiar to the Chinese and foreign students of Chinese philosophy, such as US sinologists.[718] But it is a concept hardly ever encountered by others not in these categories.

William H. Mott IV and Jae Chang Kim, authors of *The Philosophy of Chinese Military Culture: **Shih** vs. Li*, write that ***shi***h was the defining theme in *The Art of War* and that "the essence of ***shih*** was the dynamic power that emerged in the combination of men's hearts, military weapons, and natural conditions."[719] Thus, while the significance of ***shi*** is clear to major writers and translators, what is exactly meant by ***shi*** is not! Further, if these scholars consider ***shi*** to be the key and defining theme of the *Art of War*, then analysts should pay attention to the term and investigate why it is of such significance to these scholars and linguists.

Ralph Sawyer writes in his edited version of *The Seven Military Classics of Ancient China* that ***shih*** is "a measure of the relative power an army derives from positional advantage combined with its overall combat strength." Positional advantage can include terrain, firepower, morale, superior provisions, and other force multipliers. The release of strategic power can vary, based on these many factors. [720] Roger Ames believes ***shih*** can be traced back to Legalist, Confucian, and even Taoist philosophical sources.[721] Dr. Michael Pillsbury, one of America's foremost authorities on the PLA and author of several comprehensive works on Chinese military thought, used his study of PLA materials to uncover several components of ***shi*** that appear key to understanding the concept:

- ***Shi*** assesses your side's potential, the enemy side's potential, weather, and geography to identify the moment in a campaign when an advantage can be gained over an opponent. ***Shi*** is a certain moment in the campaign when you could take the advantage from the enemy (He Diqing, *Campaign Course Materials*, AMS 2001);
- ***Shi*** is created in five ways, through maneuver, posture, position, psychology, and calculations. The timing and speed of creating ***shi*** in war has changed under conditions of high-tech warfare (Yue Lan, "High Tech Warfare and Contemporary Military Philosophy," *Liberation Army Daily Press*, 2000)
- ***Shi*** is the moment when it becomes apparent one side can win the war (Guo Shengwei, *Deng Xiaoping's Military Stratagems*, Central Party

718 Also spelled "***shih***"; the spelling of ***shi*** or ***shih*** used in the following pages is dependent on the spelling used by individual authors who are quoted.

719 William H. Mott IV and Jae Chang Kim, *The Philosophy of Chinese Military Culture: Shih vs. Li*, Palgrave MacMillan, 2006, p. 11.

720 Ralph D. Sawyer, *The Seven Military Classics of China*, Westview Press, 1993, pp. 429-432.

721 Roger Ames, *Sun Tzu: The Art of Warfare*, 1993, Ballantine Books, p. 281.

School, 2000)

- ***Shi*** according to the Tang founder used psycho-**shi**, geo-**shi**, and shaping-**shi** (Zhang Wenru, *China's Strategic Culture*, Beijing University Press, 1997);
- and ***shi*** can be created with stratagems (Li Bingyan, *Stratagem and Transformation*, 2004).[722]

Other definitions of ***shi*** by a host of Western sinology and Chinese experts are also available. Some of the more distinct Western definitions include the Denma Translation Group's *The Art of War*, where ***shih*** is defined as the power inherent in a configuration;[723] Francois Jullien, author of *The Propensity of Things*, who defines ***shi*** as the potential that originates not in human initiative but instead results from the very disposition of things;[724] William H. Mott IV and Jae Chang Kim, authors of *The Philosophy of Chinese Military Culture*, who define ***shi*** as the dynamic power that emerged in the combination of men's hearts, military weapons, and natural conditions;[725] and the *Military Power of the People's Republic of China*, 2007, written by a group of US authors, who define ***shi*** as the strategic configuration of power, also understood as the alignment of forces. There is no direct Western equivalent of the term, according to the report.[726]

There are a number of Chinese sources that define ***shi***:

- The Chinese book *Campaign Stratagems* defines **shi** as situation, status, and state of affairs; the combination of the friendly situation, enemy situation, and the environment; trend in affairs; the integrated situation that has an impact on the effective performance of military strength; sum of all factors impacting the performance of the operational efficiency of both sides; general confrontational situation; hub of increase and decrease in operational efficiencies of two sides; the key factor determining the rise and fall of operational efficiency.[727]
- The *Chinese Encyclopedia of Philosophical Terms* explains it as "availing oneself of advantage to gain control, a natural interest," while law is the basis for governing with ***shi***. **Shi** "changes with each passing day and

722 This information was taken from a slide presentation that Dr. Pillsbury sent to this author.

723 The Denma Translation, *The Art of War*, Shambhala, 2003, explanation of *shih* on a card sold with the book.

724 Francois Jullien, *The Propensity of Things*, Zone Books, New York, 1999, p. 13.

725 William H. Mott IV and Jae Chang Kim, *The Philosophy of Chinese Military Culture*, Palgrave MacMillan, 2006, p. 11. Mott and Kim later note that the term is also used to mean the following: threaten, manipulate, deter, power, force, influence, situation's natural features, tendency, trend, gestures, and a person's circumstances (p. 15).

726 *Annual Report to Congress: Military Power of the People's Republic of China*, 2007, US Government Printing Office, p. 7.

727 Zhang Xing Ye and Zhang Zhan Li, *Campaign Stratagems*, National Defense University, 2002.

cannot return to its former self."[728]

- **Tao Hanzhang**, a retired Chinese General, defines ***shi*** as "the strategically advantageous posture before a battle that enables it to have a flexible, mobile, and changeable position during a campaign."[729]
- Chapter Five (***Shi***) in Tao's translation of *The Art of War* translates ***shi*** as "posture of the army."[730]
- At the 6th International Symposium on Sun Tzu's *Art of War* **Li Rulong** explained ***shi*** as "acting according to the situation." "Planning and concocting power" and "selecting men and employing strategic power" have always been important subjects for study by strategists throughout the ages. "Power" is actually a kind of potential energy; once the external condition is provided, this energy will demonstrate a mighty power and become a force. Such an understanding can be allied to all fields of social practice including military affairs.[731]
- The *Xinhua Zidian* (*New China Dictionary*) defined ***shi*** as power, authority, might (abuse one's power to take advantage of others); a condition that is manifested, appearance (pertaining to the natural world [physical features of a place, terrain, precipitous mountains], pertaining to movement [posture, gesture, sign, signal], pertaining to politics, military affairs, or other areas [current situation, trend of the times, the way things are going, general trend, take advantage of circumstances to attack a fleeting enemy).[732]

Thus, the complexity of the term is clearly identifiable from the definitions. Posture of the army, strategic advantage, strategic configuration of power, the alignment of forces, availing oneself of advantage to gain control, potential from the disposition of things, momentum, energy, force, power, influence, and "holding forces with hands" were all used to define ***shi***.

Shi as a situation or disposition appears to be a reflection of a conceptualization or historical thought process. These expressions and perceptions, when studied today, imply that the Chinese expressions and perceptions are more comprehensive and holistic than their Western counterparts. The Chinese mind, it appears, has been taught by its philosophical and cultural base to first locate the disposition or setting of reality before focusing on a solution to an actual problem at hand.

As an example of this conceptualization, *The Geography of Thought* describes a simple experiment where people of Western and Oriental races look at fish in an aquarium and describe what they see. The first response from an Oriental's viewpoint

728 Ibid.

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

730 Ibid., p. 44.

731 Li Rulong, "A Brief Discussion of the 'Shi' Strategy," The 6th International Symposium on Sun Zi's Art of War, selected paper abstracts, pp. 71-72.

732 *New China Dictionary*, 1971, p. 395. Translation of the definition provided by Mr. Bart Zobel.

was a description of the environment ("It looked like a pond") whereas the Western mind was three times as likely to first mention the type of fish they saw.[733] This indicates that the Oriental mind is taking in the big picture, the disposition of things. Likewise, this propensity to examine a broader disposition appears to be reflected in Chinese theorists' descriptions and definitions of strategy, which are broader than US descriptions of the concept. Whereas US strategists focus on ideas or ways, ends, and means, Chinese strategists tend to first look at objective factors existing in the world today with reference to a particular country (level of science and technology, amount spent on defense, location of forces, geo-political setting, etc.) and how to subjectively manipulate these circumstances. The Chinese examination of strategic resources and maritime passages may well utilize the same concepts.

It is Ames, however, who appears to understand the concept of ***shi*** best and what it means for the PLA today. He noted that:

> All determinate situations can be turned to advantage. The able commander is able to create differentials and thus opportunities by manipulating his position and the position of the enemy. By developing a full understanding of those factors that define one's relationship with the enemy, and by actively controlling and shaping the situation so that the weaknesses of the enemy are exposed to one's acquired strength, one is able to ride the force of circumstances to victory.[734]

So, having explored the three components that describe how to do strategy, how are these concepts applied in conjunction with national interests in the geostrategic field?

Chinese National Interests

> *National interests "both **objectively** exist and are to a very great extent determined by **subjective** judgments."*[735]

National interests open the second chapter ("Determinants of Strategy") of the **2005** English edition (Chinese original was written in 2001) of the book *The Science of Military Strategy*. Authors **Peng and Yao** state that strategy manifests itself in the war conductors' activities of **subjective** guidance. Further, strategy is based on given **objective** physical conditions that are restricted by social modes of production and conditions of history. Many **objective** physical conditions are manifested in the form

733 Richard E. Nisbett, *The Geography of Thought*, Free Press, 2003, p. 90.

734 *The Book of War*, p. 55.

735 Li Ying, interview with Zhu Feng, "China's Core Interests are not Suitable for Expansion," *Guoji Xianqu Daobao Online*, 10 January 2011. The explanation of China's national interests provided here is presented in a year by year format. The time frame is the past decade.

of national interests.

National strategy is based on national interests with the latter serving as the start point for strategic guidance. A national interest is defined as "an aggregate of **objective** physical and spiritual requirements on whose existence and development a state depends. National interest is the cardinal basis to determine the alignment of a state's military strategy as well as the starting point and also the destination of its national military strategic guidance."[736] Two national interest classes exist: **national interests of existence and national interests of development.** Interests include national territory, national security, national sovereignty, national development, national stability, and national dignity. National territory concerns resources and living space. National security includes information, energy, military affairs, and so on.[737] Sovereignty is a state's "inherent power to have legal supremacy internally and independence externally."[738] National stability refers to a state's maintenance of normalcy and orderliness, and national dignity is a state's deserved status and prestige in the international community.[739]

However, national development is perhaps the area where China's geostrategic interests are most prominently emphasized. This dynamic component refers to a state's economic prosperity, science and technology progress, and improvements in people's living standards. Thus, searches for new markets and for oil and gas would fit this aspect of national interests. Chinese living standards are measured against those of other nations and with past calculations of China's comprehensive national power, especially those measured on the basis of economic prosperity and overall national strength.[740] Some developmental national interests are fundamental while others are long-term. On occasion, China may find commonality or an antagonism of interests with a state. In the latter case, when compromise is not possible, war can break out.

Spearheading developmental interests in the field of strategic resources is the China Development Bank. This bank is directly responsible to the State Council of China and is China's only bank whose governor is a full minister. The bank uses energy-type loans to ensure that China's energy needs are met and resourced properly. Such loans help integrate government policies with private objectives, that is, companies make money while the government pursues its core and national interests. In any case, China Development Bank is an institute that should bear intense future scrutiny as a means for pursuing strategic resources. The bank likely will play a very important role in China's energy strategy.

Peng and Yao write that Chinese national interests are in conformity with the interest of the proletariat or general mass of people. A national interest must answer the question "what is to be protected or gained?"[741] From this analogy China's leaders rationalize efforts to attain oil and gas and other geostrategic resources "for the good

736 Peng and Yao, p. 39.
737 Ibid., pp. 39-40.
738 Ibid., p. 40.
739 Ibid., pp. 42-43.
740 Ibid., p. 42.
741 Ibid., p. 44.

of the masses." The focus of geostrategy, they write, should be on long-term interests instead of immediate ones. Today, however, China's leaders must focus on both long and short-term interests simultaneously.[742] It is important, therefore, to find China's core national interests because they will offer principal clues for the detection of geostrategic plans.

Major General **Ma Ping**, the Deputy Director of the Strategic Studies Department of NDU, wrote an excellent article in **2005** on national interests and strategy. Ma stated that national interests are the starting point for strategic planning. Clearly defined national interests help determine objectives to defend and areas to keep under observation in case threats might emerge. National interests can also help sort out potential strategic partners and opponents. National interests can be divided into **core interests**, major interests, and general interests. **Core interests** are vital interests. They include sovereign independence, territorial integrity, system security, and non-endangerment of economic lifelines. A major interest includes the unimpeded channel for the acquisition and transport of resources overseas. This latter category could be the basis for China considering the South China Sea (a separate section on this area appears later in this paper) to be a core interest. Ma makes the case that major interests, due to contemporary conditions (i.e., China's need for oil), can migrate to the core interest category.[743] Over the past few months, in both open publications and in private conversations, the Chinese have stated that the South China Sea has now become a core interest. As Ma notes:

> Our per capita resource reserve levels are low to begin with; with a population of 1.3 billion and growth rates in excess of 9%, reliance on domestic resources alone would make it difficult to support economic development, thus our dependence on foreign resources is constantly rising. At present, we depend on foreign sources for 40% of our oil. If we continue to grow at this rate, by 2010, that figure could reach 60%. Foreign dependence on other major mineral resources will also increase. By 2010, foreign dependence for iron, copper, and aluminum could reach 57%, 70%, and 80%, respectively. It can be said that the ability to securely obtain foreign resources has already begun to have lifeline significance for China's economic development.[744]

Ma notes that a nation must be militarily secure if it is going to be able to protect its national interests. A nation must be able to win wars it fights, form a strategic deterrent or counter-deterrent to an opponent's deterrence capabilities, and develop an advantage in forces or at least attain a balance of power with respect to one's opponents. These developments to ensure military security primarily are concerned with **core** and major interests.

742 Ibid., pp. 46-49.

743 Ma Ping, "National Interests and National Security," *China Military Science*, No. 6 2005, pp. 61-72

744 Ibid.

Developments in this age of military transformations are also faced with severe challenges and strategic opportunities. One of the most important challenges that must be overcome is the ability to create advantageous situations (***shi***) on China's periphery when reacting to, reducing, or resolving external military pressures. Simultaneously, a strategic opportunity has presented itself to China in the fact that China can build up its military potential and thereby develop new capabilities in the absence of conflict.[745]

With regard to **stratagems**, Ma recommends using concepts such as "feigning" and "making noise" in order to allow opponents to sense one's deterrence capabilities and determination. An opponent must be made aware of one's actual strengths and determination to use them when necessary. The credibility of one's deterrence capability is important to develop as well as the mechanisms under which deterrence functions best and is brought to true effect. With the appropriate timing and means, military deterrence can, in effect, "subdue the other army without fighting."[746] At all times it is important to maintain flexibility, applicability, and initiative.[747]

In **2006** author **Wang Guifang** discussed in a general fashion a breakout of the topic of national interests, also in *China Military Science*. Wang wrote that preserving national interests is the explicit strategic objective of China's general strategy and foreign policy. Security, he notes, is an **objective** condition in which the nation is free from danger, and, at the same time, it is a **subjective** feeling in people's minds. Security has allowed China to become more **objective** and rational in understanding its national interests. For China national interests are the start point and purpose of the country's national security strategy, whose core objective is economic development. Wang divides national interests into three levels: **core interests**, principal interests, and general interests. The description of each interest group correlates well with Ma's description of **core**, major, and general interests. **Core interests**, Wang notes, require not only economic strength but also military strength. **Objectively**, however, there is a generation gap between China's military strength and that of the world's advanced nations.[748]

Wang writes that China's national interests have become broader and now can be affected by the entire international situation. The nation must continuously reassess the importance and relevancy of these interests and also the policies of major powers toward China. An assessment of these policies leads China to formulate different policies in response. The most important responses are directed at the major powers and at the regional/peripheral geographical special environment around China, which has the most direct impact on its policies. Luckily the globalization process, in Wang's opinion, has restricted the **objective** conditions for confrontation and, instead, opened a **strategic opportunity** for attaining interests through political and economic cooperative means. He implies the use of **stratagems** against major powers when he invokes the

745 Ibid.

746 Ibid.

747 Ibid.

748 Wang Guifang, "National Interests and Choices of China's Security Strategy," *China Military Science*, No. 1 2006, pp. 76-83.

following resolve: update the rules of the game, adapt ourselves and learn the skill of implementing the competition mechanism, master the art of struggle, prudently make selections, prevent and mitigate possible crises, and achieve a new political balance. Further, do not fall into the trap of so-called "democracy."[749]

Noted Chinese strategist **Li Jijun**, using the same publication in **2006**, made several of the same points as the other authors. He noted that national interests are the starting point and objective of military strategic thinking and that the economy determines national interests. Strategic thinking, to Li, includes the processes of comparison, judgment, selection, decision-making, implementation, feedback, modification, summarization, and sublimation in the minds of those who command a war. He added that the ocean is the hope for China's future development and the nation's long-term interests; and that the confrontation of military strategies is not limited to the military domain but extends to the political, economic, scientific, technological, cultural, diplomatic and **resource domains** as well.[750]

Li used the **objective-subjective** and **stratagem** issues to buttress his arguments regarding strategic thinking. He stated that winning victories on an **objective** material foundation is stressed, while the outcome of a war is often determined by the **subjective** guiding capabilities of the two sides in a war. The **objective** conditions can change from the time before a plan is made to the time after which it is established. The **objective** condition must be continually monitored for its methodological significance if one is to resolve contradictions between it and **subjective** guidance.[751] Li then notes that the ancient Chinese emphasized the use of **stratagems** and that countermeasure-oriented thought today still utilizes **stratagems**. **Stratagems** require innovative thought. The latter is the negation of fixed models and conventions. It puts new discoveries into play, and these discoveries are what enhances and propels the art of war. **Stratagems** often employ the use of uncertainties and surprise or the use of unconventional actions, such as mixing fake actions with real ones. Li adds that the use of uncertainties is a conscious act that uses **stratagems**. Their use can resolve a dispute in the early stage of a confrontation and before the situation becomes too heated.[752] This kind of diplomatic, political, or economic use of **stratagem** should be considered by US analysts as they ponder Chinese moves in the South China Sea.

The abstract of **Kang Wuchao's 2007** article, "Analysis of National Interests and Strategic Orientation," begins with the sentence "The determination of strategic orientation is the result of the composite effects of various **subjective** and **objective** factors."[753] This focus underscores the ties of **subjective** and **objective** thinking not only to strategy but also to national interests. Kang states that national interests determine the selection of China's strategic orientation. He lists three factors that help determine

749 Ibid.

750 Li Jijun, "Military Strategic Thinking and Scientific Decision-Making," *China Military Science*, No. 1 2006, pp. 28-38.

751 Ibid.

752 Ibid.

753 Kang Wuchao, "Analysis of National Interests and Strategic Orientation," *China Military Science*, No. 2 2007, pp. 84-90.

national interests. First, territorial integrity and sovereignty are the most important factors. Second, geographic strategic interests have been growing in importance. They determine strategic orientation based on a country's goals for future growth beyond its borders. Finally, the integration of the two issues (territorial security and geographic strategic interests) reflects strategic orientation. Kang states that this concept of integration was exemplified at the beginning of the 1950s, when China decided to fight alongside North Korea against the US. China has half of its heavy industry in the northeast (territorial security) and the Korean Peninsula is a springboard for landing on mainland China. In a more contemporary example, Taiwan is viewed as a focal point for China's sovereign, political, economic, and military interests.[754]

A **2009** article in *China Military Science* by **Huang Yingxu** and **Li Ming** offered the view of two military officers on the Communist Party of China's views on national interests. National interests, they note, determine political doctrine, guidelines for action, strategy, and class or political group policies. Mao had a vision of permanent interests that corresponded to the nation's interests. National interests must embody the common interests of the Chinese people. They sit above class and special interests. The common interests of the people of China can be found in the development of social productive forces that offer a rise in living standards. Chinese strategy in all of its forms (political, military, diplomatic, and developmental) must take this common interest as its ultimate goal, according to the authors.[755]

Over time, Huang and Li add, each leader of China not only has stressed the same key items, but they have also expanded on these items in accord with contemporary developments. **Core interests** remain national sovereignty and security.[756] Mao was the leader who put state sovereignty, security, and territorial integrity above all else. Deng Xiaoping, Jiang Zemin, and Hu Jintao have added economic development, comprehensive power, and developmental interests, respectively, to this list. Deng Xiaoping stated that "national rights are more important than human rights."[757] Jiang focused on the security of strategic materials such as food and oil, as well as on information and financial security. Hu has expanded the list to include the "developmental interests" of maritime, space, and electromagnetic space issues, among others.[758] Finally, the authors state that to confront "hegemonism and power politics" China must increase its economic and military power.

Senior Colonel **Wang Guifang** was a research fellow at the Department of War Theory and Strategy Research at the Academy of Military Science when he wrote on national interests in *China Military Science* in **2009**, some three years after his first article appeared. He noted that, broadly speaking, there are two types of interests: security and developmental. National security interests are the most important element of national

754 Kang.

755 Huang Yingxu and Li Ming, "On CPC Members' Outlook on National Interests," *China Military Science*, No. 6 2009, pp. 1-11.

756 Ibid.

757 Ibid.

758 Ibid.

interests. They have always maintained an **objective** existence.[759] However, as society changes, so too does the **objective environment** and, thus, the content of national interests. Guifang focused special attention on **developmental interests**, noting that:

> It is exactly because of the more pronounced feature of development interests that the formerly self-contained security interests entered an unprecedentedly broad realm and incorporated, at the same time, certain content that had not been given serious attention before, such as closer ties with many fields of social and national life. Judging from its composition, national security interests not only include traditional military security interests and political security interests, but also include a broader range of content, including economic security interests, cultural security interests, information security interests, ecological security interests, environmental security interests, and space security interests that have become increasingly pronounced in recent years.[760]

Guifang added that **core interests** remain state sovereignty, territorial integrity, national unity, political stability, and national survival. In times of **developmental interests**, energy resource security interests and others are increasing. Perhaps this idea has been expressed most explicitly in recent conversations with Chinese officials, who have stated that the South China Sea area has become a **core interest**. In terms of geological space, Guifang notes that "sea space is more important than land space."[761]

Zhang Xiaotian, writing in **2010,** discussed the demands that national interests place on strategy.[762] Even though only a major, his article was placed first in the No. 3, 2010 issue of the journal *China Military Science*. Zhang defined national interests as "the **objective** material demand and the spiritual demand that a country relies on for survival and development. It is the starting point and the destination of a country's various acts." There are **three levels of national interest: core, key, and general**. **Core interests** are fundamental interests bearing on a country's survival, security, and development. **Core interests** affect military strategic orientations. Key interests include a country's economic development and the security of its communication channels, energy supplies, and regional interests. General interests include citizen safety, enterprise development, ecological security, and so on. General interests have the least impact on military strategy.[763]

There must be a balance between a country's strategic capabilities and the expansion of a country's national interests. Perhaps one can assume from this statement that China's new military capabilities are a result of its expanded set of national interests.

759 Wang Guifang, "An Analysis of Basic Features of and Actualized Approaches to the Development of China's Security Interests," *China Military Science*, No. 6 2009, pp. 20-25.

760 Ibid.

761 Ibid.

762 Zhang Xiaotian, "New Demands Imposed by National Interests Expansion upon Innovative Development of Military Strategies," *China Military Science*, No. 3 2010, pp. 1-7.

763 Ibid.

One cannot get ahead of the other.[764] National interests are a primary cause of war, according to Zhang. **They determine a country's strategic intentions**; are one of the five causes of war (fame, interests, evil doings, internal turmoil, and hunger); are the essential basis for distinguishing friend from foe; and impact the entire course of a war's development (its scale, intensity, length, and use of strategic weapons). National interests are the start point and destination of strategic guidance since they determine strategic situations and strategic intent. The ultimate goal of strategy is to defend or seize national interests.

These interests change, however, over time and military strategy changes with them. There are four causes for changes to national interests: developments in science and technology that result in an expanded area of reach for national interests; the rise and fall of a country's strength and status; changes in **subjective** cognition that alter the scope of national interests (based on a new understanding of a world whose direction and actions constantly change); and differing interpretations of international rules, regulations, and laws. Due to China's increased status and strength, the rest of the world should expect a sudden expansion of China's national interests, in Zhang's opinion. [765] This expansion does seem to be underway.

The expansion of national interests results in increased demands for strategic capabilities. Perhaps this is why the world is witnessing the rapid expansion of China's military force, especially its air, sea, and space components, along with strategic countermeasures.[766] National interests also influence the adjustment of strategic deployments. What all of this implies, Zhang notes, is that military strategy must continually adapt to the growing impact of the expansion of national interests in China. The country's leaders insist that development will pursue a peace-keeping resolution, insist on cooperation and win-win outcomes, play a constructive role in regional and world development, and not aim at territorial and influence expansion.[767] This sounds like a kind and humane approach to world affairs. He states:

> The development of China's national interests at the new stage in the new century is fundamentally different from the expansion of interests by Western big powers in history, and this difference is seen in such areas as the objectives, means, ways, and processes, as well as the impact produced. The factors that determine this difference not only include the influence of the **objective** strategic environment but also the results of **subjective** strategic choices.[768]

However, all of these points are contestable, the latter two particularly so. China is implementing regional development in countries that ignore basic

764 Ibid.

765 Ibid.

766 Ibid. Countermeasures may include the development of aircraft carriers, satellites, and other means.

767 Zhang.

768 Fan Zhen Jiang and Ma Bao An, *On Military Strategy*, National Defense University Book Series, 2007, p. 59.

human rights or democratic rule. Simultaneously, the Chinese label the US as a hegemonic power bent on world domination using colonial methods of enslavement, an analysis that totally ignores the US's peacekeeping work, food supplies to needy nations, and countless other humanitarian acts. It also ignores China's own history of bloody slaughter during the Cultural Revolution, problems with its own work force, and unwillingness to recognize its own support of regimes that ignore basic human rights. The Chinese suggestion that the state reject the use of influence is equally as contestable, since the use of soft power is a growing Chinese preoccupation, one based on public relations and the spread of China's cultural influence worldwide.

It should thus be expected that the greatest period of Chinese expansion may occur in the next ten years. They perceive a current window of opportunity of which to take advantage. The expansion of national interests expands national strategic interests and the space in which the leadership can maneuver. For example, China is trying to establish logistical bases abroad such as a potential port in Gwadar, Pakistan. Military tasks now include safeguarding opportunities for strategic development and safeguarding national interests worldwide.[769] On the other hand, with an expansion in the number of partners working with China (for example, in the Shanghai Cooperation Organization or SCO), relations with other nations are more complex than ever before.

Zhu Feng, the deputy director of the Center for International Strategic Studies of Beijing University, was interviewed online by Li Ying in January **2011** about China's **core interests**. He stated that he agreed with State Councilor Dai Bingguo's assessment that China's **core interests** are to maintain its social system and national security, to maintain China's national sovereignty and territorial integrity, and to maintain steady economic and social development. **Development**, Zhu noted, meant achieving secure supplies of energy and resources.

Zhu recommends a larger role for China's foreign ministry and public opinion organs. He further notes that China must use proper language and behavior and avoid "talking to ourselves and playing with ourselves" via simply trying to attain the moral high ground and repeating melancholy stances.[770] That is, public opinion must be used to buttress support for strategic interests. Reporter Li Ying, in his introduction to his interview with Zhu, noted that national interests "both **objectively** exist and are to a very great extent determined by **subjective** judgments" thereby underscoring the objective-subjective link yet again.

China's Strategic/Objective Environment

The relationship between the strategic environment and military strategy is a

769 Zhang Xiatotian, "New Demands Imposed by National Interests Expansion upon Innovative Development of Military Strategies," *Guofang* (*National Defense*), January 2010, pp. 14-16.

770 Li Ying, interview with Zhu Feng, "China's Core Interests are not Suitable for Expansion," *Guoji Xianqu Daobao Online*, 10 January 2011.

*relationship between **objective** reality and **subjective** guidance.*[771]

Before examining China's strategic resource theory it is worthwhile spending a few minutes to look at China's objective environment, the Chinese environment in which strategic resources are postulated and developed. The opening quote to this section is taken from the opening paragraph of a chapter titled "The Objective Environment of Military Strategy" in the **2007** PLA book, *On Military Strategy*. It once again underscores the close link between strategy and China's objective-subjective thought process. Key factors in the international strategic environment (political, economic, military science and technology, geography, etc.) provide the **objective** factors that determine the basic direction for building and wielding military force. **The proper assessment of the international strategic environment is the prerequisite for formulating military strategy.** Characteristics of the times (i.e., science and technology advances that influence the shape of war), the world's strategic structure (balance of power, demand for resources), and strategic trends (economic and defense policies, military deployments and alliances) of other countries all affect this environment.[772]

China's domestic strategic environment also impacts military strategy. The most immediate impact is felt in its geographic and political environment and comprehensive national strength. Geographically a **nation's security coefficient** is determined by a country's size, location, topography, weather, resources, and population. These determine the arrangement of military forces and key points of strategic defense. The political environment is determined by a nation's political qualities, policies, legal system, and basic social characteristics. Comprehensive national strength is determined by a country's economic strength, defense strength, and national cohesion. They make up a nation's total material and spiritual strength.[773]

The authors noted that there are natural geographic elements (a state's geographic position, size, and shape of territory; natural resources; national capital; national boundaries; distance between states; and grand strategic space) and human geographic elements that affect strategy. Based on these relationships, an assessment of the security environment and an orientation of a state's strategic role must be made to include judgments on the direction of the main strategic threat and a determination of the key points of strategic attack and defense. There are vital interests between states, between the interests of nations and religions, between various strategic alliances, and between geo-economic relationships that may determine the lineups of certain players.[774] Thus, a strategic study must be comprehensive, and it must view war from various aspects and stages (space, time, etc.).[775]

Economic globalization and openings with other nations have expanded the Chinese leadership's view of national strategic interests. A nation's overseas dependence

771 Fan and Ma.
772 Ibid., pp. 60-63.
773 Ibid., pp. 64-65.
774 Ibid., pp. 62-72.
775 Peng and Yao, p. 9.

on economic development and on requirements for strategic resources is rising. These requirements are hindered by the unstable economic environment and the necessity to safeguard overseas investments and sea-lane security. National strategic interests have expanded from land to the sea and from the air to outer space. Non-traditional security topics have taken on added importance, to include environmental, information, and social security issues. Chairman Hu Jintao has made the following demands on the military: assure Party dominance, secure strategic opportunities for national development, and safeguard national interests and world peace.

Military strategy's basic strategic tasks include first of all safeguarding the Party's ruling position, a task of prime importance which, to a Western mind, seems like an act of self-survival and demonstrates a lack of confidence in the military leadership. A second task of military strategy is safeguarding national unity and China's sovereignty and integrity. Deng Xiaoping pointed out that sovereignty and security must always be considered first. Containing Taiwanese independence activities occupies first place here.[776] Not only must border defense and counterattack operations be perfected, but the PLA must also "actively construct military situations that favor us in resolving disputes over border territories."[777] Constructing favorable situations is reminiscent of constructing *shi* or strategic advantage.

Contention over maritime issues is becoming increasingly intense. The Spratly Islands, the authors note, represent China's outpost and communication link to Southeast Asian countries, Europe, and Africa; are the outpost of security for China's mainland in the south; and have an enormous impact on China's economic affairs. The South China Sea has an abundance of aquatic products and large amounts of oil and natural gas resources. The East China Sea is the channel through which China must pass to get to the Pacific Ocean and the US, East Asia, and the south of Russia. It has abundant energy and fishing resources as well.[778]

A third task of military strategy is safeguarding social stability within the country and a fourth task is safeguarding the ever-expanding area of strategic interests. **China is moving from survival interests toward developmental interests.** As national interests expand, China must enlarge its effective space and defensive combat capabilities in accordance with its military strategy. As requirements for oil consumption rise daily, it becomes ever more important to safeguard maritime shipping routes. Finally, military strategy must be able to safeguard world peace, space interests, information, and science and technology developments. With regard to information, effective information defense forces must protect the country from reconnaissance and information incursions from other countries while simultaneously information offensive forces must be developed and information deterrence activities improved. World peace developments include expanding military exchanges and improving mutual military trust, strengthening regional stability, participating in United Nations (UN) peacekeeping operations, and

776 Fan Zheng Jiang and Ma Bao An, *On Military Strategy*, Beijing National Defense University Publishing House, 2007, pp. 50-54.

777 Ibid., p. 54.

778 Ibid.

promoting international arms control, disarmament, and nonproliferation pacts.[779]

Retired PLA general **Yao Youzhi**, writing in **2007** in the book *National Defense Ideas and War Strategy*, listed the elements of the strategic environment that have evolved in the 21st century. These are political multipolarization, economic globalization, and military informatization. As a military officer, Yao focused on the latter issue the most. He stated that informatization has improved the military superiority of hegemonic countries; has led to an arms race for the strategic initiative; has changed the shape of warfare; and has turned space into the new commanding elevation for international military competition. Informatized warfare depends, to a great degree, on the support offered by military space systems. Victory or defeat can depend totally on fighting for and controlling information superiority and space supremacy.[780] Yao added that traditional security threats and non-traditional security threats have become interwoven. For example, Yao writes that the US is using the argument of "counterterrorism" as a means to carry out a global hegemonic strategy through a unilateralist policy that, to a large degree, influences the international strategic situation. Of course, Yao's comments came in 2007. Perhaps now, some four years later, his tune may be different due to China's financial advances, Russia's war with Georgia, the turmoil caused by Arab Spring in the Mideast, and other factors.

Yao also discussed border disputes and maritime interests affecting China's strategic environment. First, he discussed the Sino-Indian dispute. He notes that along the 2,000-kilometer border the two nations share there are eight places of potential conflict. Three are in the western segment of the border, four are in the central segment, and one is in the eastern segment.[781] Second, he discussed the South China Sea dispute, where four large archipelagos—the Pratas Islands, Paracel Islands, Macclesfield Bank, and the Spratly Islands—are claimed by China and by adjoining countries. China's policy has been to shelve disputes and engage in joint development of the region, according to Yao. He writes:

> We need to soberly recognize that China's reefs have been occupied, its marine resources have been plundered, and the trend of 'internationalizing' the South China Sea dispute is still growing…disputes in the South China Sea will continue to move in the direction of 'pluralistic occupation of the reefs, legitimized division of the sea area, internationalized exploitation of the resources, and complicated military struggles' as intervention and involvement by international powers becomes increasingly obvious.[782]

Third, he discussed the East China Sea continental shelf and Diaoyu Island dispute. China, divided by the "Okinawa Trough" from Japan, wants the shelf divided according to the principle of "natural extension," using the centerline of the trough as

779 Ibid., pp. 55-59.
780 Yao Youzhi, *National Defense Ideas and War Strategy*, PLA Publishing House, 2007, p. 69.
781 Ibid., p. 72.
782 Ibid., p. 73.

the boundary. Japan wants to use the centerline of the sea to divide the shelf. The result is a disputed area of 210,000 square kilometers. Yao notes that the countries could still clash over the issue of oil and gas field exploitation in the area.[783] Internally, of course, China has to control supporters of East Turkistan Independence and Tibetan separatists who are continually working to stir up trouble, in China's view, in China's Xinjiang and Tibet regions.

Yao appears less worried over North Korea than Japan. He considers the latter as striving to become a military power at an alarming rate. In Southeast Asia, Yao notes an alarming arms expansionist trend in the countries of the Association of Southeast Asian Nations (ASEAN), a growth in terrorist and separatist activities in the region, and the growing intervention of powerful countries in the region's affairs. In South Asia the disputed area of Kashmir continues to fester and Yao believes the possibility always exists that peace could evaporate quickly in this region. He believes India is sparing no effort to expand its political influence at the international level. Moreover, as in other regions, the fight against terrorism remains grim. In Central Asia the rise of the "three forces" threat remains the center of focus. These are the religious extremist, ethnic separatist, and international terrorist forces.[784]

Yao provides a glimpse of the growing confidence of China's expansionist tendencies. He writes that "in the new stage of the new century, China's rapid economic development is certain to promote continual expansion into external economic spheres." Further, "security problems concerning China's access to strategic energy in particular will become more prominent." He concludes by noting that military strategy must be ready to ensure a security environment for China that is favorable to national development and economic rights.[785] Interestingly, Yao does not address Chinese expansion into Africa or South America or other areas of the globe.

Shi Yinhong of Renmin University believes that China should mainly choose bandwagoning and transcendence as diplomatic strategies. Bandwagoning means jumping on the bandwagon of a trend, abiding by international norms, and acquiring advanced technological, management, and other methodologies. This is done by forming a world relationship with other countries based on harmony and common interests. Transcendence means participating in all international security institutions that benefit China more than they cost China.[786] **Guo Shuyong** of the Foreign Languages University of the PLA stated that leader, onlooker, challenger, and partner strategies have been the historical categories of grand strategies.[787] **Ye Zicheng** of Beijing University noted that China has yet to form a full strategic system.[788]

---

783 Ibid.

784 Ibid., pp. 74-79.

785 Ibid., pp. 79-80.

786 Shi is quoted in Men Honghua, "How to Conduct Grand Strategy Studies—A Discussion of the Significance of China's Grand Strategy Studies," paper presented at a conference at Renmin University, Beijing, on 29 July 2004.

787 Ibid.

788 Ibid.

Geo-resource Issues

Thus far this paper has outlined elements of the Chinese strategic thought process, China's concept of national interests, and China's objective environment. It is now time to take these background issues and apply them to China's resource strategy. One Chinese analyst has defined a **strategic resource** as "the long-term, overall, active and constructive **materials influencing China's security and development**. The said resources include economic resources, financial resources, technological resources, information resources, and resources of professional personnel."[789] Recent Chinese articles have deemed soft military power, defense personnel, and near space as strategic resources. Strategic resources are required to maintain China's peaceful development and comprehensive national power is said to encompass "all sorts of national strategic resources."[790] Thus, when talking of strategic resources it is necessary to be precise. National strategic capabilities are said to refer to a "nation's capabilities of turning strategic resources into its strategic intention and achieving its strategic objective."

Another source defined a strategic resource as the cornerstone of national security and development; a "critical point in the geostrategic interest competition among the big powers" that needs to find expression in state policies and state behavior; and the essence of the state's future security and development.[791] The author stated that China:

> Should, according to the **objective** situation of the changes in the international environment and domestic development, redefine and make clear the status of strategic resources in our national security, direct the strategic view to the establishment of a stable strategic resources security system, strengthen the state's strategic reserve construction, increase the development and use of international resources, adjust the domestic resources consumption structure, and guard against the tendency of losing the strategic resources control direction in the course of opening up to the outside world.[792]

China's military strategic capability, the author adds, must match its national strategic status and be in line with national development interests. National strategic capability is more important than comprehensive national power since it is the shield of national security and development. It organizes strategic forces to achieve strategic objectives and represents a unity between material and spiritual capabilities as well as between strategic planning and the art of command.[793]

---

789 Chen Jiehua, *China's Diplomatic Strategy in the 21st Century*, Shishi Press, 2000.

790 Long Fangcheng and Li Decai, "On the Relation between Military Soft Power and Comprehensive National Power Plus State Soft Power," *China Military Science*, No. 5 2009, pp. 120-129.

791 Yao Xiaoxuan, "Look Squarely at the Strategic Chain of National Security and Development—Strategic Resources, Strategic Industries, and Strategic Capability," *Jiefangjun Bao* Online, 23 December 2010, p. 10.

792 Ibid.

793 Ibid.

In **1998**, in an interview with **Ku Guisheng**, a deputy Director of a Scientific Research Department at China's NDU, reporter Yu Chunguang asked about China's desperate strategic resource situation and what could be done. Ku responded that a top priority was to work out a reasonable strategy for the development and application of strategic resources. He recommended the following: to conduct a universal survey and assessment of China's strategic resources; to set up a reasonable "system for comprehensively evaluating strategic resources" and a regulation and control mechanism; to tap new natural resources and consume them in an economical and reasonable way; to improve the protection and management of strategic resources; and to institute a strategy for the exchange and replacement of natural resources.[794]

Another source, *The Science of Military Strategy*, noted in **2001** that many geographic elements form a state's geo-strategic thought process. Resources fall under the category of "natural geographic elements." Due to its size, China is able to exert its geostrategic influence well beyond its local area due to its strong political, economical, scientific, military, and technological power.[795] Further, authors Peng and Yao write:

> Natural resources are sources of means of subsistence and means of production of human society as well as the **objective** conditions on which existence and development of a state depend. Natural resources may fall into two broad classes: regenerative resources (resources of land, water, biology, etc.) and non-regenerative resources (mineral resources and fuel resources, etc.). Distribution of resources consists of land resources and maritime resources. In history plundering and controlling natural resources were always the economic root cause of war. Under modern conditions scrambling for resources is not only represented by seizure and control of land resources but also represented by that of oceanic resources.[796]

With regard to oceans, the authors write that "it is a key point of a state's geo-strategic relationship to maintain its national maritime power and rights in accordance with the United Nations Convention on the Law of the Sea (1982)."[797] Outer space is also a new and sensitive national geo-strategic relationship.[798] In order to decide when to act on China's geo-strategic relationships, Peng and Yao note that "If a state wants to make a correct strategic decision, it must at first soberly recognize and judge its position in the geo-strategic configuration and international order, and then define its own role in international relationships so as to adroitly guide its behavior according to circumstances, go after gains, and avoid harm to make maximum realization of a state's strategic interest."[799] Peng and Yao conclude this section of their book stating that

794 Yu Chunguang, "Strategic Resources Concern State Economic Security," *Jiefangjun Bao*, 25 May 1998, p. 4.

795 Peng and Yao, pp. 62-63.

796 Ibid., p. 64.

797 Ibid., p. 65.

798 Ibid.

799 Ibid., p. 68.

the interaction and mutual influence of one state on another is the result of different national geo-strategic interests. Sometimes states come together for their own ends and sometimes they come together as rivals for the same resources. States may form blocs with other states, they may remain neutral, or they may adopt an anti-alignment stance.[800] Further, different strategic geographic features will bring about different developmental orientations of strategic power.[801]

Entire books have been written on the topic of grand strategy by both Chinese and US analysts. In **2004 Men Honghua**, speaking at a conference at Renmin University in Beijing, stated that grand strategy studies are based on three variables: national strength, international institutions, and strategic concepts. The process starts, however, with an evaluation of strategic resources. Men stated that grand strategy can be defined as "the art of integrated use of national strategic resources to fulfill national security and international objectives, whereby a state uses it strategic resources and strategic means, at the political, economic, military, cultural, and ideological levels, to protect and further the country's overall security, values, national interests, and so on."[802] Men notes that the definition stresses the use, importance, and implications of strategic resources for fulfilling the objectives of grand strategy. Strategic objectives must be kept in balance with strategic resources and means.[803] Men stated that strategists must possess the professional qualities of "strategic thinking, including awareness of overall interests, foresight, knowledge of history, awareness of the big picture, grand vision, rationality, logical thinking, and the power of integration. Specifically speaking, grand strategy studies emphasize relevance to overall interests and totality before anything else and entail integrated thinking to achieve the maximum goal of the country."[804]

National strength can be measured through a quantitative analysis of a nation's strategic resources and through international comparison. National strategic resources include not only hard strength (economic and military resources) but also soft strength (strategic conception, national strategic thinking, and decision-making power). An evaluation of national strategic resources allows for an evaluation of strategic capacity, the optimization of strategic concepts, the definition of strategic objectives, and the planning of strategic content and execution of strategic means.[805] It also determines whether a country must seek strategic resources outside its borders.

Tang Yongsheng, an Assistant Director and Professor at the Strategic Studies Institute at China's NDU, penned an interesting **2008** article on strategy. He noted that there are changes to the concept of power in the international environment and the environment also has much new content due to the effect of globalization. However, China does not appear to be thoroughly probing the logic inherent in these changes,

800 Ibid., p. 71.

801 Ibid., p. 70.

802 Men Honghua, "How to Conduct Grand Strategy Studies—A Discussion of the Significance of China's Grand Strategy Studies," paper presented at a conference at Renmin University, Beijing, on 29 July 2004.

803 Ibid.

804 Ibid.

805 Ibid.

thus lowering the mandate for developing a new strategy. Further, it is not enough to equate planning national grand strategy with an extension of military strategy and equating strategic planning to a simple extension of **stratagem**. In planning national grand strategy it is necessary to regulate the use of **stratagem**. If the goals of grand strategy are correct, then optimizing **stratagem** selection in the choice of means, opportunities, and skills will undoubtedly help in the faster attainment of strategic goals. Strategists must learn to judge the hour and size up the situation, understand and adapt to new developments, and seek long-term development. The clever strategist does not rely on strength to impose his ideas on the **objective** world but rather can recognize the situation and use his own capabilities within the context provided by the logic of history. Strategic planning must encompass a more far-reaching philosophical realm that takes advantage of opportunities. China must create conditions and promote processes that lead to the country's rejuvenation, to include balancing relations with the US and building mutually constraining relationships. China's path to attain its ever-expanding set of national interests should be as much circuitous as straight, gradually accumulating the strategic initiative during a long-term interaction with the external world. The US-Japanese link should be diluted, the Sino-ASEAN link strengthened, the SCO consolidated, and the South Asian Association for Regional Cooperation (SAARC) should play a positive role in regional cooperation. Finally, China should take some bold steps and undertake international responsibilities.[806]

Zhang Minqian wrote another interesting **2008** article that attempted to get at the changes that globalization has introduced to geopolitics in general. Zhang was the Deputy Director of the International Strategy and Security Research Center at the University of International Relations when the article was written. He noted that the idea of "many winners" had taken priority over the "law of the jungle" due to the increased influence of international systems. Other issues that have impacted on the concept of geopolitics include geo-economics, geo-culture, technology power, information power, nongovernmental policies, and geo-space (regional and global geography). The composition of strategic forces is now driven by economic interests, culture, and other concepts (the role of resources, capital, nontraditional security factors, etc.) more than ever before. Small countries possessing important strategic resources are having added influence on international relations. These changes led Zhang to believe that China's strategic choices should focus first on handling relations with countries on its periphery and with the US. Second, China should champion international cooperation to deal with global and nontraditional security challenges. Finally China should attach more importance to soft power and abandon the "victim" mindset as well.[807]

Xiong Guangkai, former keeper of the intelligence portfolio as Deputy Chief of the General Staff (he retired in 2005) and currently the honorary chairman of the China Foundation for International Strategic Studies, viewed the new global security strategic

806 Tang Yongsheng, "Act by Taking Advantage of Opportunities, to Deal with the Changes," *Xiandai Guoji Guanxi*, 20 September 2008, pp. 23-25.

807 Zhang Minqian, "Geopolitical Changes and China's Strategic Choices," *Xiandai Guoji Guanxi*, 20 May 2008, pp. 18-19.

situation and environment in **2009** as in need of a comprehensive security approach. This is because issues of integration and coordination are affecting all areas (economics, science, technology, environment, politics, and the military). China should safeguard its national development and maintain the present important period of strategic opportunities.[808] Oil, food, climate, public health, information, and financial issues are the top security concerns of China, in Xiong's opinion. For example, with regard to oil issues, Xiong noted that China's approach must include "implementing a strategy of diversifying channels of energy supply, adjusting energy consumption structures, increasing strategic oil reserves, and **intensifying efforts to exploit overseas oil through international cooperation**."[809] Oil will require transportation routes. With oil China is making waves in its efforts to declare the South China Sea to be a **core national interest**, and it is exploring other sea sovereignty and maritime interest issues as well.

From this basic understanding, China's attempts to acquire resources (energy, raw materials, etc.) for its developmental needs and to secure supply routes for these resources into China should form the basis for a resource strategy. Three questions ensue: what resources do the Chinese need? Strategically, what are the **objective** factors of China's resource strategy (the what and the where)? What are the **subjective** factors involving their acquisition and transport? In the end, does the acquisition of these resources fulfill the **developmental interests** and needs the Chinese seek? **Developmental interests** and needs may be for the good of the populace, for the attainment of military advantage, or for a host of other issues. For the remainder of this paper any strategic resource reference is to strategic energy or mineral resources.

Two strategic resource issues will be addressed in more specific detail below. The external resource that is of concern to Chinese national security is oil. The issue of China's strategy to obtain oil access in Sudan will be covered in particular, as well as the resources transportation route to China, that is, the South China Sea issue. The internal strategic resource of China that affects other nations is rare-earth elements, of which China currently controls more than 90% of the world supply. China's strategy in regard to this resource, a strategy that has not been extremely successful of late, is also covered. The reader is reminded that this unclassified look at China's geostrategic concerns offers few glimpses of thinking from above, that is, the opinions of China's top leadership. Rather, the examination is based on articles and books produced by journalists. However, their thoughts are quite revealing and worthy of examination as good examples of Chinese strategic thought.

African Oil

Energy resources are always a resource of the first rank. They represent the primary motivation behind any developmental strategy, whether it be for the citizen (oil for cars, electricity for home heating and cooling, etc.) or the military (fuel for tanks, ships, and aircraft, etc.). The impetus for China's quest for energy resources, especially oil, is

808 Xiong Guangkai, *International Situation and Security Strategy*, Foreign Languages Press, 2009, pp. 133-139.

809 Ibid., p. 143.

based on China's large and growing population and its dwindling supply of domestic oil reserves. China's three best-known oil corporations—China National Petroleum Corporation (CNPC), China Petrochemical Corporation (Sinopec), and China National Offshore Oil Corporation (CNOOC)—are all working diligently to bring black gold back to China.

Chen Bo's 2005 article, "On Strategic Resources and National Security," in *China Military Science* addressed China's energy concerns, using petroleum as a case study. Chen wrote that without a stable supply of strategic resources a country does not have complete national security. Strategic resources help ensure economic growth, political stability, and military security. Petroleum is the most important strategic resource since it is "a key factor for creating social wealth, for making scientific and technological progress, and for supporting and winning victories in war."[810] It is "the basic driving force for industrialization and an industrialized society."[811] Since oil resources are unevenly distributed (sometimes in contested areas), obtaining essential supplies has become a critical national security issue. Whereas much of today's oil supplies are found in an arc from Northern Africa to the Middle East to Central Asia, the Asia-Pacific region is short on oil resources.[812]

With resources located in areas other than the Asia-Pacific region, Chen stresses the importance of securing routes for the import and export of resources. He writes that "those who control the oil transportation routes will actually hold dominance over oil resources in that specific region."[813] This situation could make maritime and pipeline transport the focal points of future rivalries between countries. The Strait of Malacca between Malaysia and Indonesia is important for China since it links the Indian Ocean with the South China Sea and is a main passageway for transporting oil to China.

China's rapid modernization will increase its demand for oil. Since 1993 China has been an oil importer. In 2005, Chen stated that China had 21% of the world's population, its economy accounted for 12% of the world's total, but its oil resources accounted for only 2.3% of the world's total. Thus, China's demand for oil is increasing yearly. Chen predicted that China's oil demand will be 300 million tons in 2010, 400 million tons in 2020, and 500 million tons in 2050. With this situation in mind, Chen notes that "it is necessary to make proper strategy and policy adjustments as soon as possible to guarantee national security in this regard" and "it is necessary to redefine the status of strategic resources in China's national security according to the changed **objectiv**e situation of the internal environment and China's domestic development."[814] Not surprisingly, Chen states that China must speed up developing a credible maritime security guarantee and its diplomatic efforts must focus on this issue as well. China must establish stable relations with resource-rich countries, sign bilateral and multilateral resource supply agreements where possible, and take part in international

810 Chen Bo, "On Strategic Resources and National Security," *China Military Science*, No. 1 2005, pp. 7-15.

811 Ibid.

812 Ibid.

813 Ibid.

814 Ibid.

cooperative organizations. Further, Chinese diplomats should explore risk-sharing and comprehensive development issues with resource-rich countries. More specifically, China should:

- Expand its economic and political influence in the Middle East, Central Asia, and South America
- Increase those people's understanding of China
- Build up a benign environment favorable to China's import of oil
- Have Chinese petroleum enterprises internationalize business contact with Asian, African, and Latin American countries
- Become a balance to the influence of Western transnational groups.[815]

Chen also feels that China should advocate, promote, and participate in the building of an energy source cooperative supply system in Northeast Asia and in a long-term mechanism for guaranteeing the effective supply and security of strategic materials. Internally China should establish a state strategic resource security system that includes the state's strategic storage system, the development of domestic and overseas resources, and the strategic adjustment of the domestic resource consumption structure. Oil storage should not fall below one quarter of the annual net import volume of oil.[816]

In another **2005** article, this time from the *China Daily*, **Zhang Weiping**, an associate chief economist at CNOOC, noted that leading powers such as the US adjusted their energy strategies to fit contemporary circumstances. This included expanding security resources and transportation routes. The paper stated that "the United States has managed to strengthen its strategic position in the Middle East in the wake of the Iraq War and increased threat deterrence along oil transportation passages through its military presence. At the same time Washington has reinforced control over global strategic resources via giant multinationals' activities worldwide."[817] These issues—military presence and a deterrence posture over transportation routes—appear to be key ingredients of China's oil strategy, as the information below will demonstrate. How widespread this thinking goes is unknown but it is apparent that many Chinese analysts believe the US went to war with Iraq simply because the latter posed a danger to the stability of the US's oil market. Will the Chinese use this rationale to go to war themselves over similar energy concerns? Hopefully it will not.

Zhang then made two rather bold suggestions. He stated that China should undertake the following steps: (1) prospecting (involving huge risks but potentially handsome returns and acquisitions) for gas fields and oilfields should be undertaken simultaneously; (2) tapping into energy resources in countries that have backward oil and gas infrastructures (while helping them establish their own energy industries)

815 Ibid.

816 Ibid.

817 "China Needs Sophisticated Overseas Energy Strategy," *China Daily* (Internet Version), 7 November 2005.

should be pushed simultaneously. This helps ensure a win-win situation in which both parties are able to share the benefits. In hindsight, China has done just that in African countries.

China's strategy, according to one **2005** article, is to use military measures as a backup only, to take advantage of new technologies, funds, and management superiorities, and to satisfy Chinese needs in countries other than those controlled by developed countries. This strategy includes developing greater resource diplomacy, energy diplomacy, and state diplomacy to create the political and economic environment and a safe external environment (sea routes?) for Chinese companies to go global. Further, China must move away from its dependence on Middle East oil and diversify its imports. It must participate in organizations with influence over the international energy investment scene to create more favorable conditions for its foreign policy ventures.[818]

Xiong Guangkai notes that China is now the world's second largest oil consumer.[819] He further writes that in **2006** British Petroleum's World Energy Statistics stated that global oil reserves "would only last another 40 years or so if their exploitation was kept at the current speed, while natural gas and coal reserves would only last 65 or 162 years respectively."[820] For China, maintaining sustained development and overseas access to this diminishing domestic resource (oil) have become vital strategic challenges.[821]

Africa, of course, has been a focal point for Chinese strategic activities for some time. A **2006** report stated that these strategic activities differ from the US approach to the region in a significant way. China is making a huge investment in infrastructure, medical service, and so on. The Chinese accuse the West of simply making accusations against the local government and imposing sanctions. The West, this report stated, hopes to kill off the "illness" (poverty, corruptions, etc.) at one blow while China hopes to "improve local immunity."[822] China's Ministry of Foreign Affairs, also in 2006, stated that "we will not act like the western colonialists in barbaric plunder and bloody violation of human rights."[823] China, on the other hand, "improves local human rights by developing the local economy through cooperation with local oil companies."[824] Poverty must be eliminated and sanctions do nothing to help this. This line of Chinese reasoning, of course, would be seriously tested if placed against US standards. It is well-known that the US has accused China of violating human rights and supporting corrupt dictators for years in Africa.

A major reason for China's interest in African oil is that most members of the continent are not members of OPEC and thus "not subject to OPEC production restrictions."[825] Further, African nations admire the rapid growth of the Chinese

818 Chen Baosen, "Calmly Deal with New Trends in the Struggle for Global Resources," *Jingji Ribao*, 17 January 2005, p. 7.

819 Ibid., p. 186.

820 Ibid., Xiong Guangkai, p. 187.

821 Ibid., p. 85.

822 Xie Yanjun and Wu Xiaopeng, "China's African Blueprint for Share Oil," *Shiji Jingji Baodao* (Internet Version), 8 May 2006.

823 Ibid.

824 Ibid.

825 Ibid.

economy, while Africa offers China a diversified energy supply channel that is fairly reliable and safe. One uses the term "fairly" due to the occasional kidnapping or use of armed gangs to extort money from foreign workers and local governments. Chinese policy makers, however, tend to ignore these difficulties (civil strife, famine, ethnic conflict, etc.) and hope to capitalize on the exodus of some US and European oil companies.

Another potential strategic issue, one at odds with traditional Chinese policy, is the easing of China's nonintervention policy toward other nations. **Wu Lei** and **Lu Guangsheng**, Professors at Yunnan University, stated in **2008** that adjustments in the principle of "non-intervention in internal affairs" offer several benefits. These include new diplomatic ideas that agree more completely with reality and the further improvement of the practicality and flexibility of China's diplomatic policies. Such adaptation will only be partial, of course, and not total. Influence can be attained more moderately through multilateral mechanisms, UN diplomacy, backstage diplomacy, and public diplomacy.[826] Wu and Lu completed their recommendation for more adjustment in China's foreign policy by noting that adjustments would be "good for enlarging China's national interests, good for the long-term overall interests of African oil-producing countries, and good for embodying China's international responsibility and international image…"[827] Obviously, this recommendation could counter one of China's Five Principles of Peaceful Coexistence (mutual respect for the sovereignty and territorial integrity of other nations) if taken too far.

In **2008 Zhao Zhiming**, the executive president of the China Petroleum and Petro-Chemical Industry, stated that China hopes to practice the principle of mutual benefits in developing African oil. The formula for success to date, according to Zhao, has been to first altruistically offer assistance, then send people to provide on-site training, and then run joint ventures with African countries and further train local talent. Technical support is buttressed with offers of financial assistance.[828] Chinese authors believe that such cooperation is based on efficiency, equality, and mutual-trust. This slow approach not only keeps Africa interested in China and lessens fears of being manipulated but also helps firm up long-term partnership packages. Moreover, there are many countries with which to implement this policy. To date, China has oil agreements or talks with Algeria, Angola, Chad, Congo, Egypt, Equatorial Guinea, Ethiopia, Gabon, Kenya, Libya, Niger, Nigeria, Somalia, Sudan, Tunisia, and Uganda. Geographically these countries are located in Africa's core area and north/northeast coast (see map at end of Appendix Two).

In **2010 Sun Xuefeng** and **Wang Haibin**, identified only as two Chinese scholars, wrote a lengthy article for *Dangdai Yatai* on China's crude oil strategy. The article is full of interesting insights and implications about the objectives and methods of Chinese

826 Wu Lei and Lu Guangsheng, "Some Reflections on the Development of Sino-African Energy Relations," *Shijie Jingji Yu Zhengzhi*, 14 September 2008, pp. 52-58.

827 Ibid.

828 Wang Guoqin, interview with Zhao Zhiming, "Thirty Percent of China's Crude Oil Comes from Africa," *Shiji Jingji Baodao* (Internet Version), 19 March 2008.

oil strategies. The authors note that, in light of China's growing demand for oil to satisfy the growing number of people and industries with energy needs and demands, a "go global" strategy was adopted in 1997. The effort has met with successes (such as the CNPC projects in Sudan) and failures (CNOOC's inability to acquire Unocal Corporation being the most publicized). Based on these experiences, however, a methodology was reached on the types of strategies and tactics to use to gain access to oil.[829]

The authors contend that a key to entering an oil-rich area is to ease resistance. That is, instead of stirring up confrontation (read "not worrying about corruption or human rights violations") or resorting to the use of force (read "no Iraq"), China should not take any initial action that would force the other side to make concessions. The strategies involved to limit confrontation and encourage participation involve the limited sharing of profits and the elimination of obstructions posed by one's rivals (again, read "US insistence that countries adhere to human rights demands"). By exploiting contradictions between China and other rivals, China can make inroads in some nations that the US and other nations cannot. Using contradictions, the authors note, means "using the strategic contradictions and political differences within the party that owns the resources or between the party that owns the resources and other rivals to secure oil development rights."[830] In summation, Sun and Wang contend that the strategies used by China to gain access to an overseas oil resource and participate in its exploitation are the strategies of limited diversion, limiting returns, and contradiction exploitation, as mentioned. To stabilize and even expand its oil in-terests in a nation China has developed three strategic initiatives. They are:

- Follow a strategic orientation, which means maintaining and enhancing China's influence over the resources owner through security protection. This "strategy requires the nation [China] to possess a substantial military power." Perhaps therein lies one significant reason for China's growing military power.

- Strengthening ties with the resource owner by providing political support and economic aid or by establishing trade contacts.

- Using the draw of technology to upgrade existing oil exploration and recovery methods in the country and thereby boost returns on development to maintain and expand China's influence.[831]

Interestingly, when discussing the stabilization and expansion phase of strategic operations, the authors cited the CNPC's successful strategy in regard to Sudan. The examination was made "in conjunction with strategic theory." The basic objective is

829 Sun Xuefeng and Wang Haibin, "China's Strategic Options at Tapping the World's Crude Oil Resources," *Dangdai Yatai*, 20 January 2010, pp. 57-78.

830 Ibid.

831 Ibid.

to increase ones influence in the resource-rich area, eliminate obstructions from competitors, ensure parties who own the resources adhere to energy cooperation policies, and protect and expand the nation's oil interests. The "protect" issue usually involves the use of the armed forces, either traditional or non-traditional (such as peacekeepers). The methods to influence nations include forming a military alliance with the resource-rich nation, maintaining good political and economic relationships with the nation to protect one's crude oil interests, and raising the level of oil development technology and recovery efficiency.

Sun and Wang note that nations that want another country's resources are inclined to take risks. If China offers support and protection to a resource-rich nation, then other countries with an interest in these same resources may resort to confrontation with China. Strategic judgment must be used in balancing the pros and cons of offering protection or not offering it. Sun and Wang believe that Chinese actions in Sudan demonstrate an aspect of this paradox. In 1995 Sudanese President al-Bashir asked China to help develop its oilfields. The initiative was prescient since the US pulled out of Sudan the following year (the authors did not say WHY the US pulled out and imposed sanctions on Sudan). By 1999 the Chinese had put its first overseas oilfield officially into production mode, and it continued to win contracts for new developments in Sudan over the next five years. In 2005 a subsidiary of China's CNPC began off-shore prospecting and entered Sudan's natural gas sector as well. Today, a little over a decade of effort has resulted in the CNPC creating a complete and comprehensive oil industry "covering production, refining, transportation, and sales and marketing. CNPC's projects in Sudan have become the company's largest and most profitable projects in Africa."[832] Thus, while not engaging the US in direct confrontation, in this case China took advantage of US policies.

Both China's technological and political support of Sudan lie at the heart of its success story. Regarding technological advances, the authors state that China has built the world's first delayed coking facility for processing high-calcium and high-acid crude oil; and with another technology it can remove sand from oil and overcome problems caused by high levels of calcium, acid, and stickiness. CNPC has also made twelve times the number of oil field discoveries than Occidental Petroleum made in a similar time frame, according to the authors. Politically, China has supported Sudanese sovereignty in the face of international pressure over the Darfur issue. In 2007 China became the first country to put forward a dual-track strategy of parallel progress, combining the search for a political solution with peacekeeping operations. China does not approve the involvement of the International Court of Justice, nor does it support internationalizing the Darfur issue. Finally, China opposed the imposition of sanctions on Sudan. Sanctions would only lengthen and worsen the conflict, in China's opinion.[833] Thus, China's approach is the inverse of the US focus on human rights and sanctions for events such as Darfur.

Concluding their remarks, Sun and Wang note that every large nation's oil interests

832 Ibid.

833 Ibid.

are enhanced if the nation can lower any resistance from its competitors and win the support of the country owning the resources, and then stabilize and expand its oil development interests in the country it is occupying. Limited diversion is a strategy for sharing overseas oil interests. It is the ideal and most realistic choice, Sun and Wang state, because it is a gradualist approach that can ease any strategic misgivings of the resource owner. In fact, the authors state that such an approach was not used when CNOOC attempted to buy Unocal outright. It might have been better just to buy some Unocal shares. The other two strategies—limiting profits and exploiting contradictions—effectively diffuse obstructions from China's rivals. Among other strategies that China may use to increase influence in a resource-rich area are providing the resource owner with security protection and maintaining a good economic and political relationship with the owner. China's energy diplomacy also relies on maintaining a close trading relationship with the resource owner and raising the level of oil exploration and recovery technology in the owner's country.[834]

The shortcoming in China's current situation is its lack of strategic influence, in the author's opinion. They finished their article noting that "fundamental to any effort to boost and enhance China's ability to obtain overseas oil interests is the expansion of China's strategic influence so that even more countries voluntarily support China's policies and so that we can prevent other countries that desire to damage China's interests from achieving their objective."[835] Therefore expect Chinese attempts to expand their influence to continue to develop.

Transporting Oil: the South China Sea Issue Heats Up

> *In past decades, the Chinese Navy's activities have been surrounded by the United States with layers of "island chains" and its energy security is controlled by the United States and other marine powers. This fact makes Chinese people concerned. In the past two days, eleven warships of the Chinese Navy sailed through the restriction of the "first island chain" from international waters to "deep blue." This news quickly became a favorable topic discussed by the Chinese people…*[836]

A current contention between China and a host of other countries (Vietnam, Philippines, Malaysia, etc.) focuses on the issue of sovereignty over strategic maritime passageways in general and over territories of the South China Sea in particular. This section discusses the issue of strategic maritime passageways from China's perspective and the issues that confront it in the South China Sea. Included in the discussion are responses from Chinese scholars, government officials, and military personnel. The essence of the discussion is that China's strategy must rely on bilateral discussions to

834 Ibid.

835 Ibid.

836 Unattributed article, "Imperative for China to Break Out of the 'First Island Chain'," *Wen Wei Po* Online, 10 June 2011.

solve these issues and not on the use of international courts and multilateral talks; must be ready to employ military force if diplomatic talks fail; must win the international media battle for influence over public opinion at home and abroad about the correct position and right of China's concerns and its judicious approach; must limit concessions; and must limit or neutralize US moves (US reconnaissance missions in the area of the South China Sea, military exercises with China's neighbors, etc.) in the region. The discussion covers the years 2010 to the present.

One of the more recent and useful Chinese articles on maritime passageways was a **2010** article that appeared in *China Military Science*. Author **Liang Fang**, a senior colonel at NDU's Strategy Office for Teaching and Research, outlined the historical importance of strategic maritime passageways and how their control enabled the US to become a world power. For China, he added, energy production is now located in regions separate from the mainland, thereby making transport a key security issue. Without a doubt, Liang added, "safeguarding the security of strategic maritime passages is one important aspect of fighting for and controlling strategic resources."[837] Sea supremacy for sea powers such as the US was the result of their ability to control maritime communication lines and strategic passages while establishing maritime hegemony. Liang implies that China's view of **objective** reality is that the nation cannot supply its own energy needs and must build a naval force to secure safe passage for the products they require.[838]

Further, Liang adds that the "law of distance attenuation" in geography (the farther the distance from a target the less control over it) demands that the development of technologies, the development of regional and global alliances, and the development of overseas bases become increasingly important ways to help control and lessen the distance factor. Bases in general also serve as a strategic deterrent factor and allow for fast reaction capabilities to protect important passageways. Finally, bases protect a nation's interests and enable the protection of straits, waterways, and even open seas. Liang then states that three factors allow for the acquisition of sea supremacy in the modern age:

> The first is relying on land bases, the second is relying on island bases, and the third is relying on aircraft carriers. Of these, islands have the functions of both land bases and aircraft carriers. They are both an unsinkable aircraft carrier and an extension of land bases out in the deep sea; they can greatly expand the range of sea control. For the most part, islands must be occupied first for [protection against] offensives against the mainland. Islands are also a protective screen for the mainland, being on guard against invasion from the sea.[839]

---

837 Liang Fang, "An Analysis of the Laws of Sea Powers Contending for and Controlling Strategic Maritime Passages," *China Military Science*, No. 5 2010, pp. 135-142.

838 Ibid.

839 Ibid.

Islands are relay stations and stepping stones. They figure into a nation's **geostrategy** and receive consideration when examining national interests. In that regard islands are like small countries. Major powers frequently try to bring smaller countries located near strategic passages under their in-fluence. Such arrangements work for both countries, the larger country receiving the basing it requires and the smaller country receiving added security protection.[840] For several of these reasons China has focused its diplomacy on attaining control of several islands (Spratlys, etc.,) in the South China Sea.

Cao Wenzhen, who is associated with the Law and Politics School of Ocean University in China, added another **2010** opinion to the strategic passageways discussion. He highlighted the continuing importance of geopolitics in the age of globalization. The geographic location of strategic resources and the continuing importance of trade and supply routes almost guarantee that **geostrategy** and geopolitics are two topics that will be with us for a long time to come, in his opinion. For example, as China becomes a sea power there will be a corresponding impact on the **geostrategy** of the US, whose only bases in the region are in Japan, South Korea, and Diego Garcia. Chinese Major General Luo Yuan defined sea power as "a country's ability to control oceans by means of military power, of which the strength of its navy is the most direct embodiment, while what image a navy presents when safeguarding its sea power depends on the country's clear positioning of its navy's functions and definitions."[841] Wang Yizhou, a Vice Dean at the School of International Studies of Beijing University, stated that "it can be predicted that in the future the Chinese Navy would have increasingly bigger formations to go beyond the 'first island chain' with increasingly advanced equipment to conduct exercises so as to protect China's maritime passages and preserve international peace."[842] To counter China, Cao believes the US is attempting to build an island chain of deterrence from Japan and South Korea in the north, "through the Taiwan Strait, the South China Sea, the Philippines, and Singapore in the middle to Australia in the south."[843]

Yang Zhen and **Zhou Yunheng**, two PhD students at Fudan University's School of International Relations and Public Affairs, offered a contrasting **2011** view to the importance of sea strategy. They wrote about the growing conflict between the US and China over sea power. With regard to relations with the US, the authors suggested reasons that either conflict or cooperation could evolve from the confrontation. For conflict, he noted that the two countries have different strategies, national interests, and ideologies. For cooperation, he noted that the rise of nontraditional security issues and the deepening of integration and mutual reliance on one another have offered more room for mutual agreements. The US's strategic goals are now simply maintaining dominance instead of seizing dominance, as well as hindering China's

840 Ibid.

841 "Imperative for China to Break Out of the 'First Island Chain'"

842 Ibid.

843 Cao Wenzhen, "US-China Marine Geopolitics and Strategy in the Era of Globalization," *Taipingyang Xuebao*, 25 December 2010, pp. 45-51.

growth. The US wants unhindered power on the sea, a goal that China is challenging. China is a world trade power that increasingly relies on a secure and stable global maritime system. Ensuring the security of transportation routes from Africa and other nations is of supreme importance. To effectively control the sea China must increase its maritime strength and develop its sea power. In the mid 1980s China proposed a strategy of coastal water defense, which is a strategy of regional defense.[844] Now, due to the increased importance of transportation routes, China must expand this strategy beyond the immediate region.

The conflict between China and the US over sea power is increasing in intensity, scale, and key areas. With regard to key areas, the South China Sea is one of the most important, in the authors' opinions, for several reasons. First, several international maritime routes cross this area, to include China and Japan. Second, the internationalization of the Nansha (Spratlys) problem is becoming more acute. Third the South China Sea area is vast and is even home to some Chinese nuclear submarine bases. Finally, the area will be home to the Wenchang Aerospace Launch Center (Hainan Island), making US control of the area a way to deter China's secondary nuclear attack strength. **Objectively**, the role of armed conflict as a tool to protect national interests between great powers has declined. **Subjectively**, both nations are working hard to avoid a large scale conflict. Military engagement exercises and the development of a US-China hotline have helped this endeavor. Hopefully more work will occur between the nations over issues such as maritime terrorism, ecology, the spread of disease, trans-national crime, narcotics smuggling, illegal immigration, and piracy. However, sea supremacy is but one aspect of contemporary comprehensive supremacy. Now space and electromagnetic supremacy are as important, if not more so, than sea supremacy.[845] Perhaps for this reason China is so focused on developing its system of systems operational capability.

The products China requires to ease some of its energy needs are located far from its shores. Nearly 70 percent of China's foreign trade volume is now realized through maritime transport. Reacquiring lost territory (i.e., Taiwan) also requires sea access, according to Cao. Thus China must depend on sea routes for both economic and strategic reasons. To prevent the US from blocking Chinese access to either of these strategic targets China must continue to modernize its military, especially its naval forces. A major power, Cao notes, combines actual strength with **geostrategy** and the application of force at key strategic points. Sea supremacy is now a **geostrategic** objective that will be used to get parties to cooperate with the principle of "setting aside sovereignty and jointly developing."[846] China's future will be decided by applying the proper set of tools to its perception of **objective** reality and not by listening to "people's peace-loving subjective desires."[847] The country must develop issues of mutual

844 Yang Zhen and Zhou Yunheng, "Conflicts over Sea Power between China and the United States, *Xiandai Guoji Guanxi*, 20 February 2011, pp. 6-11,

845 Ibid.

846 Ibid.

847 Ibid

trust with the US while simultaneously preparing for the worst to avoid being caught unprepared.[848]

In May **2011**, reporters **Wen Zhizhong**, **Tang Anhua**, and **Sun Bingxian**g reported on a Guangzhou Military Region meeting with various commanders. They discussed the importance of the strategic opportunity that currently lies before the Chinese. Commander **Xu Fenlin** of the military region noted that the military must continuously take **development** as the primary requirement in this **strategic opportunity period**. **Development** must take place around the national sovereignty and security aspects of the international situation. National unity and territorial integrity are **core interests** of the state, Xu noted, and a long-term **development strategy** will enable the attainment of the initiative in world affairs. Enhancing deterrence through enhanced operational capabilities such as the system of systems capability is an achievable goal and one that will make the force capable of performing diversified military tasks. The Guangzhou Military Region lies next to the South China Sea, and China must, in Xu's words, "truly build this strategic direction into the motherland's harmonious and tranquil southern frontier making it as impregnable as bedrock."[849]

Author **Xu Zaihua** continued the South China Sea discussion in a **2011** *Jiefangjun Bao* Online article. He noted that a marine strategy with Chinese characteristics is needed to win the current fight over marine resources and passageways. The task of China's naval forces is to make preparations for actual military struggles; safeguard the country's resources and islands; strengthen control over important straits; and protect the safety of maritime transportation lines. Further it is necessary to integrate civilian and military resources and develop the capabilities for maritime transportation support using system of systems operations based on information systems.[850]

Clearly, these opinions from Liang, Cao, Xu Fenlin, and Xu Zaihua indicate that China is intent on making its navy both powerful and capable of protecting its sea lanes for economic and historical (Taiwan) reasons. China realizes that at the present time the US controls much of the strategic passageways around the country. This arrangement works fine in peacetime, the analysts note, but it also allows the US to control China if a conflict erupts. China wants to change this equation in its favor.

In drawing up its strategy for the South China Sea, **Zhu Chenghu**, a professor at NDU, stated that the effort should be led by the China Institute for Marine Affairs under the State Oceanic Administration. Other agencies, namely the military, the Ministry of Foreign Affairs, the Ministry of Public Security, the Ministry of Commerce, the Ministry of Agriculture, and the Ministry of Transport, Customs, and Coastal Provinces should also participate in the discussion. The issues of territories, the demarcation of sea borders, and maritime rights and interests should be incorporated into the discussion. Other nations in the region, in Zhu's opinion, are turning the

848 Ibid.

849 Wen Zhizhong, Tang Anhua, and Sun Bingxiang, "Guangzhou Military Region Organizes Exchange of Results in Studying and Implementing Chairman Hu's Important Expositions on National Defense and Armed Forces Building…," *Zhanshi Bao*, 12 May 2011, p. 1.

850 Xu Zaihua, "Strategic Passages are Laid Here," *Jiefangjun Bao* Online, 29 June 2011, p. 10.

South China Sea into "an ATM machine" as they plunder oil resources, open up areas to tourism, and claim land. To counter these moves, China should explore for and extract oil and natural gas off the Nansha (the Chinese name for the Spratly Islands) Islands; open the islets to tourism; make full use of the UN mandate to expand existing facilities on the Yongshu Reef, and strengthen its research in various fields, turning it into a UN research center; strengthen exploration and investigation in the South China Sea waters; and strive for greater discourse over the fate of the region. With regard to the latter issue, an information briefing mechanism should be established that will update academic institutions on recent happenings. Finally, Zhu notes that China "has indisputable sovereignty over the South China Sea despite the fact that China is the first to propose a joint development…"[851] China must understand that other nations believe they too have several sovereignty claims in the South China Sea that are backed up historically.

Chinese scholars have offered a number of opinions on how China should treat challenges to its interests in the South China Sea. In another **2011** article summarized below, seven authors were interviewed. Their ideas are varied and worth of consideration:

- **Zhou Fangyin**, Chief of the Editorial Office of "Contemporary Asia-Pacific Studies" of the CASS Institute of Asia-Pacific Studies: China should no longer make concessions or try to freeze talks or shelve disputes. Rather, China must never be ambiguous on matters of principle that require a firm stand.

- **Li Jinming**, Professor with the Research School of Southeast Asian Studies at the School of International Relations, Xiamen University: first, public opinion must be enlightened and propaganda on the South China Sea issue should be distributed. Articles should be published in foreign English-language journals. Seminars on the South China Sea issue should be convened to gain the initiative over world opinion. Foreign companies should not be permitted to explore for oil in the South China Sea. We should not allow the South China Sea issue to become international or multilateral.

- **Li Guoqiang**, Deputy Director and Research Fellow at the CASS Borderland History and Geography Research Center: there are only diplomatic, military, and legal approaches to the South China Sea issue. If all parties agree to the Declaration on the Conduct of Parties in the South China Sea a diplomatic agreement is possible. However preparations should be made to recover the occupied islets and reefs at an appropriate time if diplomatic matters don't work out. The US must be kept out. As a strategy that could be employed against the US, if a US company

851 Zhu Chenghu, "China Can Do More in its Handling of the South China Sea Dispute," *Huanqiu Shiao* Online, 1 July 2011.

participates in oil exploration then strategically it "may face tremendous losses in its interest as well as its future development in China and may even face sanctions."

- **Rear Admiral Yin Zhuo**, military expert: territorial divisions and the sovereignty of islets and reefs is the core of the South China Sea issue. Only when a country "has sovereignty over islands and reefs would it be entitled to territorial waters and an exclusive economic zone." Some countries professing to have such rights in actuality do not.

- **Ye Hailin**, Chief of the Editorial Department of South Asian Studies of the CASS Institute of Asia-Pacific Studies and Special Commentator of *Guoji Xianqu Daobao*: China's media have not gone beyond the stimulus-response model. We are only adept at following up on the reports of others and responding with statements. The media must create topics regarding what China should do in the critical South China Sea area. The media must let people know that a peaceful development may not work.

- **Gao Zugui**, Professor at the Research Center for International Strategic Studies at the Central Party School: China must not allow the US to become the arbiter over the future direction in the South China Sea. China is stronger now and this implies that neighboring countries will be more anxious and insecure. We must not allow our neighbors to undermine the stable framework that China has built with ASEAN. New discoveries may await us if we use the perspective of regional or national strategy.

- **Xu Ke**, Assistant Professor with the Institute of Nanyang Studies at the Institute of International Relations, Xiamen University: China must move out of its current passive position and look for other ways out and seek a new starting point. Combating pirates in the South China Sea can be a starting point, for example.[852]

A **2011** CCTV interview with **Yin Zhuo** and **Ye Hailin** provided an opportunity for these gentlemen to expand a bit on their views. Yin stated that of the 50-plus inhabitable islands in the South China Sea China controls only eight. Claims over the islands increased in the 1970s when oil was discovered in the region. Ye stated that China should attempt to differentiate between those ASEAN members who are willing to cooperate with the mainland versus those who try to seek every possible (economic, strategic, resource, etc.) advantage at China's expense. If concessions are made then other nations will be more provocative as well.[853]

852 Huang Yingying, "South Sea Stratagems: Standing Firm on Diplomatic Front and Drawing Support from the Media," *Guoji Xianqu Daobao* Online, 25 July 2011. All items in this bulletized format are from this article.

853 CCTV-Xinwen, 17 June 2011.

The authors of the seven interviews listed above (the three reporters) stated that China is intent on conducting a "People's War in the ocean," using military maneuvers in the South China Sea to show its neighbors that China exercises full sovereignty over the area. The security of Mischief Reef and sovereignty over the Nansha Islands within the nine-dotted line are the areas of current concern. With regard to the line, three other authors (**Liu Bin**, **Zhang Lu**, and **Fang Shuo**) wrote the following in **2011**:

> Why China's boundary line in the South China Sea is called the nine-dotted line can be dated back to 1947 when the Territorial Administration Section under the Ministry of the Interior of the Chinese government plotted an undefined line made up of eleven dotted-lines on the Location Map of the South China Sea Islands published by it. The government of the People's Republic of China also has plotted a line in the same position on maps published by it but revised the eleven dots to nine dots.[854]

These reporters wrote that China's military presence in Nansha includes the South China Sea Fleet, which is also stationed at Zhubi Reef, Nanxun Reef, Yongshu Reef, Chigua Reef, Dongmen Reef, and Huayang Reef. More than ten departments are currently exercising marine law enforcement at this time. There are five specific forces involved in this effort: the Maritime Police of the Border Control Department under the Ministry of Public Security; the Marine Surveillance Teams of the State Oceanic Administration under the Ministry of Land and Resources; the China Maritime Safety Administration under the Ministry of Transport; the Chinese Fishery Administration of the Fishery Bureau under the Ministry of Agriculture; and the Anti-Smuggling Police of the General Administration of Customs. Unfortunately the coordination among them is weak, according to the reporters.[855]

The reporters state that the only agreements with regard to the South China Sea dispute are the United Nations Convention on the Law of the Sea, passed in 1982, which is the basis for the 200-nautical-mile exclusive economic zones along the coast of neighboring countries; and the Declaration on the Conduct of Parties in the South China Sea in 2002, where signatories agreed to "exercise self-restraint in the conduct of activities that would complicate or escalate disputes."[856]

At the moment, the fishing industry has become a major point of contention among parties to the dispute. Fishermen from all nations are casting their lines in waters that are contestable with certain of their neighbors. Chinese fishing boats are required to install Beidou satellite positioning systems so that the Chinese government and patrol boats will know where they are located at all times.[857]

In a wide-ranging **2011** CCTV interview other regional and military experts

854 Liu Bin, Zhang Lu, and Fang Shuo, "China's Real Presence in the South China Sea," *Nanfang Zhoumo* Online, 21 July 2011.

855 Ibid.

856 Ibid.

857 Ibid.

offered their opinions on the South China Sea issue. **Rear Admiral Zhang Zhaozhong**, the well-known military expert and professor at NDU, states that a recent US-Vietnamese military exercise was unprofessional and a publicity stunt. **Jin Canrong**, Deputy Director of the International Relations Institute at Renmin University, stated that Vietnam intends to use the US as its "big brother," since it is the only way for the country to engage in a show of force. Jin, due to the US's domestic woes, regards America as an undependable ally. A video clip is then shown of joint exercises between the US and Malaysia, Indonesia, the Philippines, Brunei, Vietnam, Singapore, and Thailand. Zhang believes these exercises are designed to show US support for these nations over the South China Sea issue, while the real aim is to contain China. This is the US's main goal, in his opinion. He notes that Singapore and the Philippines are likely future military installations for the US. Japan is also very interested in the South China Sea because it serves as the passageway for Japan's energy needs.[858]

There are four misunderstandings regarding China's policy on the South China Sea, according to **Xing Guangmei**, a Beijing scholar writing in **2011**. First, China does not claim sovereignty over the whole of the South China Sea waters.[859] China declares sovereignty only if necessary but never advocates the use of arms. China is devoted to advancing ties with all regional actors.[860] Its claim has three points:

(1) China has sovereignty over all the reefs and territorial seas in which they are located, within the nine lines of demarcation. China's Declaration of the Territorial Seas (1958), Law on the Territorial Seas and Contiguous Zones (1992), and the diplomatic statement that "China has indisputable sovereignty over the South China Sea islands and adjacent waters" provide a legal basis for such claims.
(2) China enjoys sovereignty and exclusive jurisdiction over the exclusive economic zone extending 200 nautical miles from the territorial sea baselines along the continent and the territorial sea baselines of qualified islands and the continental shelf extending not more than 350 nautical miles within the nine lines of demarcation as a signatory of the United Nations Convention on the Law of the Sea (1982).
(3) According to the provisions of the 1982 Convention and Law on the Exclusive Economic Zone and the Continental Shelf (1998) concerning historic rights and the relevant rulings of the International Court of Justice, China enjoys priority in such historic rights as fishing, freedom of navigation, and maritime administrative law enforcement in waters outside China's exclusive economic zones but within the nine lines of demarcation.[861]

858 CCTV, 17 July 2011.

859 Xing Guangmei, "Four Major Misunderstandings about the South China Sea Issue," *Huanqiu Shibao* Online, 28 June 2011.

860 Ho Fan, "China and Vietnam Agree to Peacefully Resolve the South China Sea Disputes," *Wen Wei Po* Online, 27 June 2011.

861 Xing Guangmei.

Second, China has the right to take back occupied reefs with force or by peaceful means. Third, there should be no outside intervention in solving the South China Sea issue. Bringing in powers from outside the region will only increase their appetite for interests and will harm trade contacts. Finally, exploitation in cooperation with China will alleviate contradictions. Those who want to intensify contradictions will suffer the consequences.[862]

Professor **Zhang Zhengwen** of the Nanjing Army Command College issued another **2011** hard-line approach to solving the South China Sea issue similar to Xing Guangmei. Zhang noted that the establishment of moral principles, credibility, rules, and "awe" are required as countermeasures. The South China Sea is one of China's **core interests**, in his opinion. This means that on issues of principle there is no room for compromise. China should increase its military presence and form a strong deterrent force so that other countries will not try to cause trouble in the region. If necessary, China should launch punitive attacks when provoked and safeguard China's sovereignty over the South China Sea. If the issue is to be settled once and for all, dialogue and negotiation should be tried first followed by judicial proceedings. If these fail then force should be used.[863]

In contrast to these hard-line approaches there were softer suggestions. One suggestion appeared in a **2011** article by **Kuai Zheyuan** who noted that there are three keys to solving the South China Sea issue. They are to acknowledge the presence and interests of the US in the South China Sea; to allow ASEAN to know that China will not threaten ASEAN but will protects its safety on land and in the South China Sea; and to bring peaceful solutions to disputes over the South China Sea with Vietnam, the Philippines, Malaysia, and Brunei through bilateral negotiations.[864]

Rare-earth Elements

This section looks at an internal Chinese strategic resource, rare-earth elements, a product for which China leads the world in the extraction and processing. The section will examine the rationale behind China's decision to limit rare-earth production and exports in the past few years and the strategies of China to manage rare-earth elements.

According to Chinese sources, the country has been developing its rare-earth industry since **1968**.[865] US rare-earth expert Cindy Hurst notes that rare-earth elements (REE) are "those chemical elements on the periodic table having atomic numbers 57 through 71 (known as the lanthanides), scandium, and yttrium (atomic numbers 21 and 39)."[866] These elements are not rare but are difficult to find in high enough concentrations to make them economical to extract from the earth's crust. They are used, according to Hurst, in "hundreds of high-tech applications, including

862 Ibid.

863 Zhang Zhengwen, "In Its Handling of the South China Sea Issue, China Should Adopt Countermeasures that Focus on 'Four Establishments,'" *Huanqiu Shibao* Online, 11 July 2011.

864 Kuai Zheyuan, "no title provided," *Yazhou Zhoukan*, 17 July 2011, p. 40.

865 Cui Ning, *China Daily* Internet Version, 21 January 1998.

866 Cindy Hurst, "China's Ace in the Hole: Rare-earth Elements," *Joint Force Quarterly*, Issue 59, 4th Quarter 2010, p. 122.

critical military-based technologies such as precision-guided weapons and night-vision goggles."[867] In **2011** *The New York Times* listed the rare-earth elements found in a Toyota Prius: diesel fuel additives (cerium and lanthanum); UV cut glass (cerium); glass and mirror polishing powder (cerium); LCD screen (europium, yttrium, and cerium); sensors component (yttrium); hybrid electric motor/generator (neodymium, praseodymium, and dysprosium, terbium); headlight glass (neodymium); 25+ electric motors throughout the vehicle (neodymium magnets); catalytic converter (cerium and lanthanum); and hybrid NiMH battery (lanthanum and cerium).[868]

The Jiangxi, Fujian, Guangdong, Hunan, and Guangxi Zhuang regions are the areas in southern China that are rich in medium-heavy rare-earths. The ion-absorbed rare-earths, or medium and heavy rare-earths, are more valuable than lighter rare-earths found in the north, due to their scarcity and wide use in more advanced technologies, according to Lin Donglu, Secretary-General of the Chinese Society of Rare-Earths.[869] Most of the mining licenses for rare-earths in Jiangxi Province are owned by Ganzhou Rare-Earth. The Aluminum Corporation of China Ltd (Chinalco) is set to take a controlling stake in the state-owned Guangxi Nonferrous Metals Mining Group. Along with the Grirem Advanced Material Company the three will together form a joint venture to develop rare-earth resources owned by the Guangxi Rare-Earth Development Company.[870] Northern companies are also being consolidated. A 2011 report notes that the Inner Mongolian Baotou Steel Rare-Earth High-Technology Company is aiming to consolidate thirty-five rare-earth mining operations by June.[871] The Baotou Rare-Earth Development Zone (built in 1990) in Inner Mongolia, north China, is the primary location for rare-earth resources in China. In **1997** there were close to 145 domestic and overseas companies located there.

In **1998** China had 36 million tons of proven reserves of rare-earth, nearly 80 percent of the world's total.[872] It was number one in the world in rare-earth output and had nearly 6,000 people involved in research. Their work has resulted in the introduction of rare-earth into the metallurgy, machinery, oil, chemical, textile, and light industry sectors. Export volume surpassed 30,000 tons in 1996, which was some 65 percent of the world market. [873] Today, the US Geological Survey (USGS) believes that China has 55 million metric tons of reserves or some 48 percent of the world's reserves.[874] China undoubtedly has many more researchers of rare-earth than the 6,000 employed in 1998.

In **1999** the State Development and Planning Commission of China proposed four

867 Ibid.

868 Karl Russell, "Many Want Rare Earths, But Few Are Mining Them," *The New York Times*, 6 February, 2011, p. 7

869 Zhou Yan and Zhang Qi, "Biggest Players to Rule Rare-Earth Sector," *China Daily* Online, 20 May 2011.

870 Zhang Qi, "Chinalco Obtains Rare-Earth Rights," *China Daily* Online, 12 April 2011.

871 Zhang Qi, "Rare-Earth Giant Takes over 35 Smaller Miners," *China Daily* Online, 3 June 2011.

872 *Xinhua News Agency*, 0802 GMT, 28 November 1997.

873 Cui

874 See http://minerals.usgs.gov/minerals/pubs/commodity/rare_earths/mcs-2011-raree.pdf.

measures to promote the rapid growth of rare-earth products: to exploit deposits in a rational way (to protect China's riches in Baotou and in southwest China's Sichuan province); to expand rare-earth marketing and applied technologies (permanent magnet materials, permanent electric motors, etc.); to restructure China's rare-earth industry and reorganize its assets for better product mix; and to reap better economic returns by relying on science and technology.[875] That same year the Land and Resources Ministry of China decided to restrict the further exploitation of rare-earth elements by halting or sharply cutting the issuance of new mining licenses.[876] Perhaps this was because in 1998 China had exported 44,000 tons of rare-earth, almost one and a half times its export rate in 1996. This was 70 percent of the world's total consumption, while China's domestic market only consumed 15,000 tons. At the same time China continued to encourage foreign investment into the processing of rare-earth.[877]

There are a number of rare-earth enterprises in China, with some sources reporting as many as 130 companies.[878] While not specified, it is believed the majority are mining and not processing companies. In **2002**, North China's Inner Mongolia Autonomous Region announced a plan to build a "Rare-Earth Valley" in Baotou city. The project would consist of five parks: education, science and technology, pioneering, industrial, and logistics. More than half of the income from the park is expected to be generated by the rare-earth industry.[879] In **2004** the China Southern Rare Earth (Group) Corporation was cited as a key rare-earth firm that had merged some twenty companies, to include the Jiangsu, Guangdong, Jiangxi, and Hunan Provinces and Shanghai; and the China Northern Rare-Earth (Group) Corporation was a merger of producers from the Inner Mongolia Autonomous Region, Gansu, Shandong, and Sichuan Provinces in which the Baotou Steel and Rare Earth Company will have ninety percent of the rare-earth reserves. Thus, there was a huge movement to merge many rare-earth producers into a few larger organizations. State legal entities will have a controlling stake in both. Two large companies, the Gansu Rare-Earth Corporation and the China Rare-Earth Holdings based in Jiangsu Province and Hong Kong, declined an invitation to join the two conglomerates. This is not surprising since the government plans to grant export quotas for the two groups. Further, the government has stated its intentions not to grant new licenses to other companies within three years of the launch of the two big groups, and they intend to speed up efforts to ban those rare-earth plants without government-issued mining licenses.[880]

By **2007** Chinese analysts were calling for more strategic uses of rare-metal and rare-earth elements. Some of the actions requested were:

- Establish an operating mechanism and system for developing mines that

875 *China Economic Information Network*, 13 April, 1999.

876 *Xinhua News Agency*, 0722 GMT, 29 May 1999.

877 *Xinhua News Agency*, 0135 GMT, 20 June 1999.

878 Gong Zhengzheng, "Country's Metal Makers to Merge," *China Daily* (Internet Version), 2 February 2004.

879 *Xinhua News Agency*, 17 September 2002.

880 Gong.

both meet market economy requirements and standardize the development of mineral resources.

- Improve the strategic material reserve system in the country.
- Predict the supply and demand status of strategic materials.
- Accelerate site inspections and the development of rare metal resources.
- Expand channels for gaining resources and utilizing these resources.
- Allow newcomers to act as coordinators and managers, especially organizations such as China Rare-Earth Industry Association.[881]

The following suggestion was also put forward, and it appears to be the most realistic (and aims to be the most manipulative):

> In order to safeguard national security and accelerate the sustainable development of the national economy, we should attach great importance to rare metal resources from a strategic perspective and we should improve our ability to use our dominance of rare metals to enhance our influence in the international community and improve our ability to regulate the market so as to gain a bigger voice in the international community. In addition, we must make it clear that rare metals are a valuable trump card held by our country. We should promote resource-based diplomacy, particularly with Japan and the US.[882]

Another **2007** Chinese tactic was to prevent companies from selling rare-earth elements too cheaply. A 15 percent export tax on rare-earth elements was imposed. Earlier China had cancelled a tax rebate policy on rare-earth elements, but export volumes continued to rise, forcing the government into the export tariff plan.[883] In **2009** the European Union and the United States jointly complained to the World Trade Organization about China's export tariffs and restricted quotas on rare-earth materials. Such measures provided Chinese industries with a substantial competitive advantage in the rare-earth market. China, for its part, defended its policies and said it would consult with the concerned nations.[884] An economist in Shanghai wrote that China's decision to limit rare-earth elements is not the same as imposing a ban on them. However, the analyst offered some advice as well. He believes China should set limits to the export of its national strategic resources and increase as much as possible the export of finished

881 Zhou Shijian and Wang Lijun, "A Strategic Analysis of the Current Status of Rare Metals in Our Country," *Zhongguo Zhanlue Guancha*, 1 January-28 February 2007, pp. 52-60.

882 Ibid.

883 "China Increases Export Duties on Rare Metals," *Renmin Ribao* (Internet Version), 30 May 2007.

884 Qiu Wei, "WTO Case against China Gathers Steam," *Global Times Online*, 24 June 2009.

goods.[885] Protecting rare-earth resources and the environment helps insure that China's economic sovereignty remains intact.[886]

Meanwhile, rare-earth industry downsizing continued. In late **2008** China proceeded to construct the China Minmetals Rare Earth Company, which aimed at becoming the largest global rare-earth enterprise in the world within five years. The Ganzhou-based company was a subsidiary of China Minmetals Corporation and two private companies, the Hongjin Rare-Earth Company and the Dingnan Dahua New Material Resources Company.[887]

In August **2009** the Chinese Ministry of Industry and Information Technology (MIIT) published a "Revised Program for the Development of Rare-Earth Industry 2009-2015." The article deemed MIIT the main policymaker and regulator of China's rare-earth industry. The program was necessary to manage and regulate the more than 1,000 rare-earth deposits in China. The program divides China's rare-earth mines into three zones. The South Zone covers Jiangxi, Guangdong, Fujian, Hunan, and Guangxi; the North Zone covers Inner Mongolia and Shandong; and the West Zone covers Sichuan. For the 2009-2015 period, light rare-earth elements will be extracted from Inner Mongolia and Sichuan and, potentially, Shandong. Heavy and medium elements will be extracted from Jiangxi, Guangdong, and Fujian. The program indicates that the state will not grant new mining rights, ratification will be provided by MIIT and not a provincial-level authority, and city-level government agencies will not have the right to approve rare-earth applications and processing enterprises.[888] One source in 2009 even indicated that China's rare-earth reserves had fallen from 85 percent of the world's total to 58 percent.[889]

Rare-earth elements, of course, are viewed as a strategic trump card in some Chinese circles. A **2010** article, for example, indicated that should US companies participate in arms sales to Taiwan, then China, backed by legislation, could ban rare-earth element sales to the US. China also has indirect options, such as imposing tariffs on US parts suppliers who want to enter the Chinese market or simply deny them access. China could also enter into destructive competition against US companies on international markets. Still, reducing rare-earth quotas seems to be the way to really strike back against the US.[890] There have been other points of contention and stress with the US, however. In **2003** for example, the Gansu Tianxing Rare-Earth Functional Materials Company was involved in the illegal acquisition of Terfenol-D, used in US naval and aerospace sensors and weapons, through the espionage efforts of Chinese

885 Lu Ning, "China Restricts Strategic Resources Exports: Justified and Bold," *Beijing Qingnian Bao* Online, 29 June 2009.

886 Tao Duanfang, Ji Shuangcheng, Qing Mu, Liu Yang, Wang Xin, and Xiao Da, "China's Rare-Earth Makes the West Nervous," *Huanqiu Shibao*, 3 September 2009, pp. 1, 6.

887 "China Aims to Build Largest Global Rare-Earth Enterprise," *Xinhua News Agency*, 26 February 2009.

888 "Revised Program for the Development of Rare-Earth Industry 2009-2015 Completed," *Zhongguo Touzi Zixun Wang*, 15 August 2009.

889 Lan Xinzhen, "Resource Restrictions Not Rare," *Beijing Review* Online, 17 October 2009.

890 Wang Dake, "Consider Banning Sale of Rare-Earth Materials as Sanction against US Companies Involved in Arms Sale to Taiwan," *Dongfang Zaobao* Online, 4 February 2010.

students living in the US.[891]

China has already used rare-earth elements as a bargaining chip from a Western perspective. In the autumn of **2010** a Chinese fishing boat collided with a Japanese Coast Guard boat. This happened in the Senkaku Islands in the East China Sea and the incident was filmed by one of the Japanese Coast Guard's crew. In response to Japan's decision to hold the Chinese fishing boat captain during the investigation, China halted the export of rare-earth metals to Japan, which seriously cramped the plans of the auto and other industries. China cut its rare-earth exports to Japan on 21 September **2010** and to the US and Europe on 18 October. Beijing claims they had begun adjusting their policies before the trawler incident.[892] Some Chinese authors state that a quota system was in place in 1998 while in 2006 the country stopped granting new rare-earth mining licenses. In September **2010** the State Council put rare-earth companies on a merger list. Some nations accused China of monopolizing resources and using rare-earth as a means for exerting political pressure.[893] Chinese actions in regard to the trawler incident did one thing for sure—it sent a shock wave of concern to countries that had come to rely on China for their rare-earth supplies.

The embargo did not work well in the end for China. The stoppages triggered a harsh response from other nations. Many began to look elsewhere for rare-earth elements and some, like the US and its Molycorp Minerals LLC at Mountain Pass, California, continued with their plans to restart old mines. The positive side is found in events such as the recent (8 August **2011**) Third China Baotou Rare-Earth Industry Forum, held on 8 August 2011. One point of discussion was whether China can enhance further cooperation between itself and foreign companies that also specialize in rare-earth elements. While China is projected to have 48% of the world's rare-earth reserves, Baotou has 80 percent of China's reserves. Meanwhile, China yearly continues to provide 90 percent of the earth's rare-earth metals.[894]

In **2010**, according to one US article, China produced 130,000 tons of rare-earth elements, while the US produced zero tons. India was second with 2,700 tons, which demonstrates figuratively the world's reliance on China. According to the same article, China leads the world with 55 million tons of rare-earth reserves, with Russia second at 19 million tons and the US third at 13 million tons.[895] Chinese Premier Wen Jiabao stated in October 2010, shortly after the trawler incident, that the nation will not use rare-earth resources as a bargaining chip, even though most nations had by that time already made up their minds that China had done so. The *China Daily* Online

891 Ray Cheung, "Firm Alleged to Be Conduit for Theft of US Technology," *South China Morning Post* (Internet Version), 6 August 2003.

892 Wang Zhaokun, "Pentagon Sees no Rare-Earth Crisis, *Global Times* Online, 1 November 2010,

893 Lei Min, Wang Jianhua, and Zheng Qian, "China will Cut Rare-Earth Exports next Year, but Not by a Very Large Margin," *Xinhua Asia-Pacific Service*, 2 November 2010.

894 "China Economic News in Brief, Shanghai Auto Industry Fund, Rare-Earth Forum, John Deere Engine Plant," *Xinhua News Agency*, 30 June 2011.

895 Scott Canon, "The Race for Rare-Earth," *The Kansas City Star*, 14 June, 2011, pp. 1, 8. Another source, http://minerals.usgs.gov/minerals/pubs/commodity/rare_earths/mcs-2011-raree.pdf, listed the Commonwealth of Independent States as in second place and not Russia.

attempted to explain China's rationale regarding this issue. It noted that rare-earth elements must be cut and prices raised due to environmental problems that stem from producing 90 percent of the world's needs and from the proliferation of small rare-earth companies in China that have allowed the business to sell rare-earth at very low prices at the expense of added pollution. These two elements, over-exploitation and poor mining habits, have caused China to reduce the number of companies and set state prices and quotas. The nation is also implementing restrictions in accordance with laws and regulations. Meanwhile, other large industrialized nations such as the US are not mining any rare-earth elements and are thereby saving their reserves for a rainy day.[896] Further, rare-earth elements are used for military purposes and this is another reason for implementing restrictions on their export. This is a legitimate security concern of China. Chinese authors such as Jin Gaisong, Vice Director of the International Trade Department of the Chinese Academy of International Trade and Economic Cooperation, state that this tactic (limiting sales from Western countries to China for security concerns) has been used against them repeatedly.[897]

According to a report in **2011**, the Chinese government is setting rare-earth-element quotas based on rare-earth output, market demand, and the need for sustainable development. This system is needed. Between 1996 and 2005 rare-earth exports increased ten times and the price dropped 36 percent. In 2009 China had only 36 percent of the world's rare-earth reserves, as compared to 43 percent in 1996. Today China is closing hundreds of smaller mines (the Ganzhou production base in Jiangxi Province once had 1,035 licensed mines) and imposing a 15-20 percent tariff on rare-earth exports.[898] Prices are skyrocketing. An average ton of rare-earth exports cost $36,297 in January 2011, but by March the price was $68,305.[899] Japan has had to increase the price of its domestically produced rare-earth magnets, one of its main products, since the prices of neodymium and dysprosium, the key raw materials in the magnets, have risen sharply over the past few months. Simultaneously, Japan is trying to keep its auto and electronics industries from being held hostage by Chinese pricing. It has produced a series of actions to thwart such Chinese moves.[900]

China's rare-earth strategy appears to be composed of several aspects: first, China seems intent on producing more finished products in the rare-earth field and getting Western nations to buy them instead of raw rare-earth elements. This will provide more income for China and produce more jobs. The nation is focused on developing the entire industry chain in a strategic manner, according to Chinese Rare-Earth Society Secretary-General Lin Donglu.[901] Second, China is interested in inviting foreign high-

896 "China Wise to Guard its Rare-Earth Wealth," *China Daily* Online, 20 October 2010.

897 Jin Baisong, "Regulation of Rare-Earth Exports Needed," *China Daily* Online, 24 November 2010.

898 Hu Yue, "Even Rarer," *Beijing Review* Online, 18 January 2011.

899 Eric Ng, "Beijing Sets Production Limit for Strategic Metals," *South China Morning Post* Online, 25 April, 2011.

900 "Rising Rare-Earth Prices Hitting Downstream Industries," *Business China* Online, 8 June 2011.

901 Zhou and Zhang.

technology companies to move to China to set up shop and thereby be closer to rare-earth resources (but also become another input for the job market, as well as a potential Chinese takeover objective). In 2009, General Motors established the headquarters of its international operation in Shanghai.[902] Chen Zhanheng, director of the Chinese Society of Rare-Earths, noted that rising rare-earth prices could force some industries to transfer from Japan to places where there are rare-earths in abundance.[903] Third, the government is consolidating the scattered rare-earth sector in order to gain more influence over global market pricing and to pave the way for more sustainable growth. Finally, the State Council is allowing China's biggest domestic companies to dominate and lead the industry.[904] This is a different approach to bringing the industry under more state control than has been attempted in the past.

Simultaneously, several issues continue to go unresolved. Some regions are calling for a clear national strategy that sets exploration criteria for rare-earth reserves; for a national reserve system; and for policy incentives that boost technological innovation and application.[905] The State Council issued national guidelines for the development of the rare-earth industry on 19 May 2011at www.gov.cn, and several of these items of concern to the regions were addressed.[906] The guideline is said to raise rare-earths to the level of national strategic reserves for the first time, according to one source. *Business China* Online stated that a strategic stockpile system for rare-earths will be established (which could provide China with more power to influence global prices and supplies). The guideline is designed to handle multiple problems, to include illegal mining, environmental pollution, and a lack of centralization of the industry. The State Council added that the plan is to place 80 percent of the rare-earth industry of the south in the hands of three companies within two years. In the north, rare-earth production is already in the hands of the Inner Mongolian Baotou Steel Rare-Earth Company.[907] The company has announced that it will establish the Baotou Rare-Earth Products Exchange to "further regulate the market."[908]

On 28 May **2011** a researcher of the Chinese Society of Rare-Earths provided further details of the rare-earth guidelines. In addition to the three issues mentioned in the *Business China* release, the document was said to include twenty-two items for regulation. These items included stricter policies on waste emissions standards; regulations to curb smuggling; the implementation of production controls; laws designed to decrease the consumption rate of rare-earth reserves; the phasing out of inefficient energy consumption; the promotion of ways to improve separation, smelting, and application techniques; and the harmonization of the rare-earth industry with local

902 Hu.

903 "Rising Rare-Earth Prices…"

904 Zhang Qi.

905 "China Tightens Rare-Earth Regulations," *Business China* Online, 24 January 2011.

906 "China Issues Guideline to Promote Healthy Development of Rare-Earth Industry," *Xinhua* 19 May 2011.

907 Tony Zhu, "China Tightens Control of Rare-Earth Industry," *Business China* Online, 20 May 2011.

908 Zhang Qi.

economies and social development. Blame for past acts of surpassing approved output levels were laid at the doorstep of local governments that did not properly supervise private industries in the face of adequate laws and regulations according to the researcher.[909] Over the past few months, while export have dropped in total volume by some seventy-six percent, the value of exported rare-earth items has increased by 214 percent.[910] In this sense the guidelines are providing expanded income and reducing pollution as the plan was intended to do.

One other article of interest in **2011** represents China's interest in standing on its head US arguments to prohibit the sale of high-tech items to China via export restrictions and embargoes. Author Sun Yefei detailed the rare-earth elements in US military equipment and stated that he saw no reason to sell rare-earth to the US that might be turned into military equipment posing a threat to China. He wrote that the US Patriot missile's guidance system was composed of four kilograms of samarium-cobalt magnets and neodymium-iron-boron magnets to produce electron beam focusing; and that Patriot's control wings contain rare-earth alloys. Further, he detailed the rare-earth components of missile tail fin systems, the electric engines of some naval ships, and US armor's anti-penetration capability.[911]

Conclusions: Assessing the Geopolitical Impact

Many of the primary characteristics of the **objective-subjective** thought process are apparent as one proceeds through the discussions of national interests, the objective environment, oil, the South China Sea, and rare-earth above. The "how" to conduct strategy indicates the following. First, Chinese strategists look at **objective** conditions and reality via such criteria as the number of forces opposing them, the terrain, the level of science and technology in a country, a country's defense budget, and so on. This is more important than the "operational environment" which drives much US thought. The Chinese then use creativity and **stratagems** (**subjective** guidance) to manipulate these **objective** factors to their benefit. The goal is to attain "***shi***" or strategic advantage. Strategists are limited based on the economic conditions of the regime (social mode of production determines the type of weapons available) and military history and culture (social conditions of history that influence how force or diplomacy will be used and when).

However, when analyzing Chinese writings on oil and rare-earth, several different strategic topics pop up than those focused on ***shi***, **stratagems**, and the **objective-subjective** thought process. This indicates that China has significant strategic plans and operations underway but not necessarily the type that fit easily into the three paradigms offered above. Their geostrategy appears to be flexible and adaptable and willing to disregard several issues of intense value to the West (human rights, local corruption, etc.). With regard to African oil and the South China Sea, the following

909 Chen Zhanheng, "Rare-Earth Protection Plan," *China Daily* Online, 28 May 2011.

910 Shi Xiangjun and Geng Yajie, not title provided, *Neimenggu Ribao* Online, 31 May 2011.

911 Sun Yefei, "Do Not Turn Rare Earth into Thin Mud, and Let the US Military Turn Stone into Gold," *Zhongguo Qingnian* Bao Online, 26 August 2011.

strategic options emerge from the writings used for this paper:

Oil and strategy

- Using to China's benefit the strategic contradictions and political differences that exist between the parties that own resources and China's rivals
- Participating with international energy investment groups to create more favorable conditions (***shi***) for joint ventures.
- Working to "improve local immunity" in oil communities via developing the local economy instead of the US method of killing off the "illness" through sanctions and human rights
- Working with non-OPEC members of the oil industry, which limits the number of production restrictions on Chinese investments
- Making adjustments to China's "non-intervention" policy in reaction to **objective** reality
- Offering assistance altruistically, sending people to provide on-site training, and running joint ventures
- Offering financial assistance and taking actions that would not force the other side to make concessions
- Using technologies to upgrade facilities and advance returns on development
- Enhancing Chinese influence through the offering of security protection arrangements
- Using the strategies of limited diversion (sharing overseas oil interests, a gradualist approach that can ease any strategic misgivings of the resource owner) and limited returns
- Strengthening ties with resource owners through trade contacts
- Working to establish bilateral alliances with resource-rich countries
- Providing resource owners with security protection, such as placing peacekeepers in the region in case military force is needed to ensure the security of resources
- Taking risks
- Taking advantage of other nations policies that are driven by human rights or sanctions

South China Sea (transport routes) and strategy

- Establishing a military presence to create a deterrent posture over transport routes
- Developing greater resource, energy, and state diplomacy to create the political, economic, and safe external environment required for transport
- Countering what China believes is a US island chain of deterrence from Japan and South Korea to the Philippines and Singapore

- Establishing a set of coercive tools that get parties to listen to the principle of setting aside sovereignty and promoting joint development
- Making no concessions on the South China Sea issue
- Prohibiting foreign countries from exploring for oil and imposing sanctions on the US if it does so
- Establishing a public relations offensive to enlighten people on China's position
- Prohibiting the US from becoming an arbiter over South China Sea issues
- Coercing all parties to agree to the Declaration on the Conduct of Parties in the South China Sea and preparing to recover islets and reefs if diplomatic maneuvering does not work out
- Focusing on an active versus passive position, such as offering to combat pirates in the area

Rare-earth and strategy

- Consolidating the industry to rid the country of domestic rogue rare-earth companies that mine but care little about the environment and set prices lower than state prices for sales overseas
- Implementing laws and regulations to keep the nation's supply of rare-earth plentiful
- Predicting the supply and demand status of strategic materials.
- Enhancing China's influence in the international market and improving its ability to regulate the market
- Promoting resource-based diplomacy with the understanding that rare-earth is a valuable trump card that can be played when required
- Providing China's Ministry of Industry and Information Technology (MIIT) with the ability to grant mining rights, ratify mines, and approve applications and processing inquires
- Using rare-earth as a bargaining chip (this is a US understanding of Chinese rare-earth strategy, based upon Chinese actions in the East China Sea: when a Chinese fishing boat collided with a Japanese Coast Guard boat, the Chinese boat Captain was detained, and China halted rare-earth exports to Japan until the case was adjudicated); China has indicated that rare-earth shipments could be halted to the US if arms sales continue to supply Taiwan (Chinese Premier Wen Jiabao has publicly stated that rare-earth elements will not be used in this way, as a bargaining chip)
- Limiting world supplies, since other nations appear to be stockpiling rare-earth buys from China and putting them in their reserves for a rainy day
- Producing more finished products in the rare-earth field, so that other nations have to depend on China not only for rare-earth elements but also for finished products as well; holding hostage other nations' industries

with Chinese pricing
- Inviting high-tech Western companies to move to China to produce finished products, allowing China to get a high-tech infrastructure as well out of the deal
- Bringing the rare-earth industry under state control
- Turning US strategy (based on a reluctance to authorize shipments of technical equipment to China that can be integrated into its military equipment) on its head by refusing to send rare-earth elements to the West that can be used in military equipment

China's economic rise is dependent on strategic resources, especially energy resources. In addition to core, general, and major interests, China has designated the search for strategic resources as an expression of "developmental interests," a category somewhat new to the various subdivisions of national interests. At the same time that China searches for new energy resources it must find a way to reduce its reliance on coal and develop industries with a higher science and technology content thereby enabling it to become more "green." To achieve this goal China plans to devote 10 trillion yuan (about $1.5 trillion) to develop seven strategic industries over the next five years, a plan still under discussion in late 2010. These industries are alternative energies, new generation information technology, biotechnologies, high-end equipment manufacturing, advanced materials, alternative-fuel cars, and energy-efficient and environmental protection technologies.[912] It is hoped that the plan will help compensate for the rise in economic and environmental prices that China has paid for the dramatic rise in its comprehensive national power and people's welfare.[913]

With regard to information technology, China is seeking to prepare a new grand strategy with information at the center of attention according to Zhang Xinhua, editor of the book *Information Security: Threats and Strategy*. Two areas of this strategy are the science and technology area (security and safety of digital space) and the political area, where soft power rules. Opportunities abound to improve or exploit information sovereignty, information hegemony, information permeation, information domination, and information contamination in Zhang's opinion.[914] Strategic goals "can be achieved by destroying or manipulating the flow of information on computer networks to destroy an enemy's telephone networks, oil pipelines, power grids, traffic management systems, systems for transferring state funds, systems for transferring accounts, and healthcare systems."[915] This means that "the key to success may be in proficiently practicing strategic management of information capabilities. Thus what lies at the heart

912 Hu Yang, "China's $1.5 Trillion Industries Boost Not yet Official: Report," *China Daily* online, 6 December 2010.

913 Jian Guocheng, "Reviewing Restructuring in China and Looking Ahead to Development, Changing Development Model in the 12th Five-year Program," *Xinhua Domestic Service*, 23 February 2011.

914 Zhang Xinhua, editor, *Information Security: Threats and Strategy*, 2003, publisher unknown, p. 54.

915 Ibid., p. 48

of grand strategy is paying attention to information security and building and applying information strategy."[916]

In summary, China's geostrategy is developing on several fronts. Some are based on the basic principles of an **objective-subjective** analysis, the use of **stratagems**, and the end goal of achieving ***shi*** or a strategic advantage. **Objective factors** of the international situation are analyzed and assessed and a **subjective** rendering of them results in the formulation of policies, principles, and plans. However, the methods to achieve advantage are flexible and vary in accordance with the issue under consideration, as the list of strategic objectives under each category above indicates. The issue is to find a way to attain a comprehensive strategic advantage and the main goal is to position strategic objectives within the scope of national interests. It is postulated here that these three issues (**objective-subjective, stratagems, and strategic advantage**) are present in Chinese strategic planning by implication and historical tradition.

David Finkelstein, perhaps the US's finest expert on Chinese military strategy, notes that new strategic guidelines for the Chinese military are issued in response to changes in the international order; to the international or regional security environment; to China's domestic situation; and in the nature of warfare itself.[917] China's assessment of its current geostrategic situation would indicate that, even though adjustments have been made since the last guidelines of 1993, new guidelines could appear in the next year or two. The appearance of a new discussion over China's core and developmental interests support this contention.

China's needs are clear. It must acquire an abundant supply of energy to meet the requirements of its people. One of the ways is to do all it can to go to a source of oil that is not dependent on OPEC, that being African oil. In so focusing its attention on that continent, China must also secure the oil's passage through the South China Sea. Its military capabilities, especially the Navy, are being built up to support that proposition. In that sense, China's **objective** view of reality has changed since its Navy is stronger than in the past. This has resulted in **subjective** policies that will hopefully, from their point of view, provide the strategic advantage it seeks to control both the oil resource and its passage to refineries in China. Threats appear to play a prominent role as well. On 29 September 2011, Long Tao, a strategic analyst of China's Energy Fund Committee, stated in the *Global Times Online* that it was "time to teach those around the South China Sea a lesson" and that China should strike first before things get out of hand. [918] Minnie Chan discussed Long's article in the *South China Morning Post Online* on 30 September. Chan noted that some 2,000 internet users supported Long's view. Also of note was that an anonymous retired PLA colonel stated that war will be inevitable if the Philippines and Vietnam push China into a corner.[919] Thus the

916 Ibid., p. 53.

917 David M. Finkelstein, "China's National Military Strategy: An Overview of the 'Military Strategic Guidelines,'" *Asia Policy*, No. 4 2007, pp. 67-72.

918 Long Tao, "Time to Teach Those Around the South China Sea a Lesson," *Beijing Global Times Online*, 29 September 2011.

919 Minnie Chan, "Wage War in the South China Sea," *South China Morning Post Online*, 30 September 2011.

issue continues to get hotter and hotter.

Internally, China has plenty of rare-earth elements and does not need them. However, from an outsiders view, China appears to be trying to corner the market, the pricing mechanism, and the finished product industry. Internally, China had to corner its own rare-earth companies and put the industry under state control. That has been accomplished. China lacked some of the internal capabilities to process rare-earth elements and so it has sought to bring foreign companies with such capabilities into China and thus providing access to the finished product industry.

In each case, China is focused on manipulating objective reality to fit its internal situation and to obtain a strategic advantage. Thus far China's geostrategic plan appears to be unfolding in spite of the few constraints put on it. China's geostrategic approach will require close scrutiny in the coming years as China advances further as a world power. Nations must ensure they understand China's strategy if they hope to escape being ensnared by it and subjugated to it.

Articles on Strategy from 2009-2010 in the journal *China Military Science*

1-2009: A Historical Analysis and Current Development of the Thought of Military Strategies

2-2009: A Study of National Strategic Capabilities

3-2009: A Study of Military Strategic Guidance in the New Period in the New Century

4-2009: A Comparative Study of Naval Strategies of Today's World Major Powers

5-2009: On the Concept that the PLA Should Establish for Strategic Projection

6-2009: Strategic Choices of China's Defense Economy in the International Financial Crisis

1-2010: There were four articles in a special section on the "Expansion of Strategic Interests in China's Past Dynasties"

2-2010: A Tentative Analysis of Hu Jintao's Strategic Thinking on Accomplishing Diversified Military Tasks; A Comparative Study of Clausewitz's and Jomini's Strategic Theories; Closed and Open Maritime Strategies of the Ming Dynasty and their Influence

3-2010: On the Development of National Interests and the Development of Military Strategy; Strategic Thinking on Safeguarding the Development of National Maritime Interests; Challenges to Space Interests and our Strategic Choices; Characteristics of China's Traditional Strategic Thought

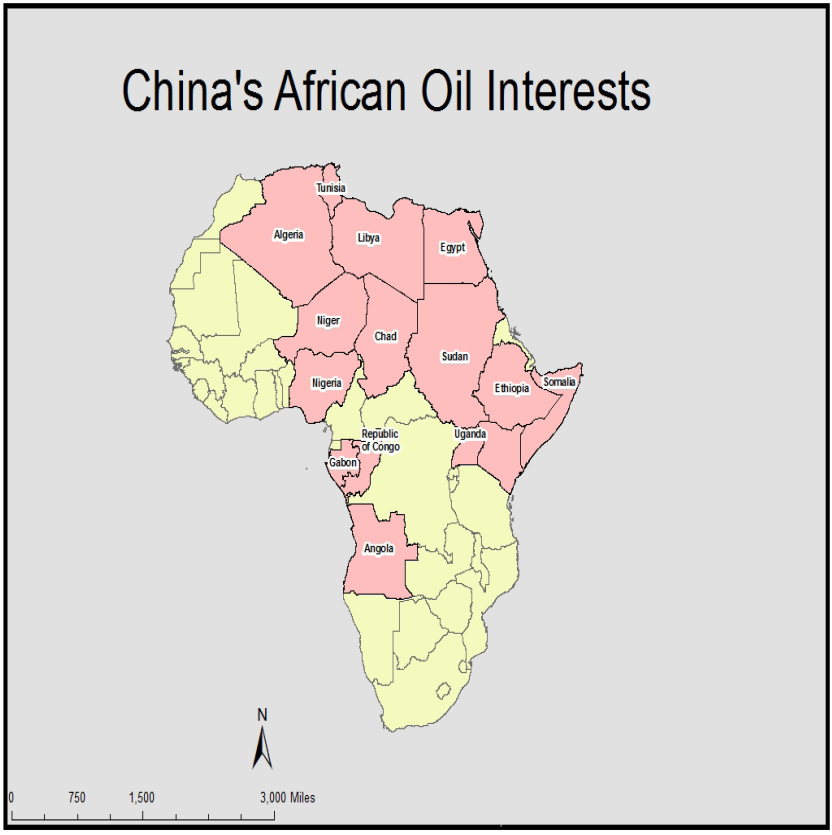
4-2010: None

5-2010: Great Strategic Decisive Battles and Famous Historic Chapters—on the Historical Position of the Three Great Strategic Battles during the War of Liberation in 1948-1949

6-2010: Fundamental Strategy for Scientific Building of a Powerful Army in the New Stage in the New Century—Theoretical Significance and Practical Value in Hu Jintao's Strategic Thinking on Improving the PLA Capability in Dealing with Multiple Security threats and Fulfilling Variable Military Missions; Fundamental Strategy for Building the PLA into a Powerful Iron Army—Studying the Newly Revised *Regulations of the PLA on Political Work*; A Summary of Research on China's Grand Strategies; A Grand Panoramic Display of Military Strategic Thinking—An Introduction to *A Study of Contemporary Military Strategic Thinking.*

Map of Countries in Africa

from which China is Extracting Oil



ABOUT THE AUTHOR

Mr. Timothy L. Thomas (BS, Engineering Science, USMA; MA, International Relations, University of Southern California) is a senior analyst at the Foreign Military Studies Office at Fort Leavenworth, Kansas. Mr. Thomas conducts extensive research and publishing in the areas of peacekeeping, informa-tion war, psychological operations, low intensity conflict, and political-military affairs. Mr. Thomas was a US Army foreign area officer who specialized in Soviet/Russian studies. His military assignments included serving as the Director of Soviet Studies at the United States Army Russian Institute in Garmisch, Germany; as an inspector of Soviet tactical operations under the Commission on Security and Cooperation in Europe; and as a brigade S-2 and company commander in the 82nd Airborne Division. He has written four books, three on China and one on Russia, on information warfare topics. Mr. Thomas is an adjunct professor at the US Army's Eurasian Institute; an adjunct lecturer at the USAF Special Operations School; and a member of two Russian organizations, the Academy of International Information and the Academy of Natural Sciences.