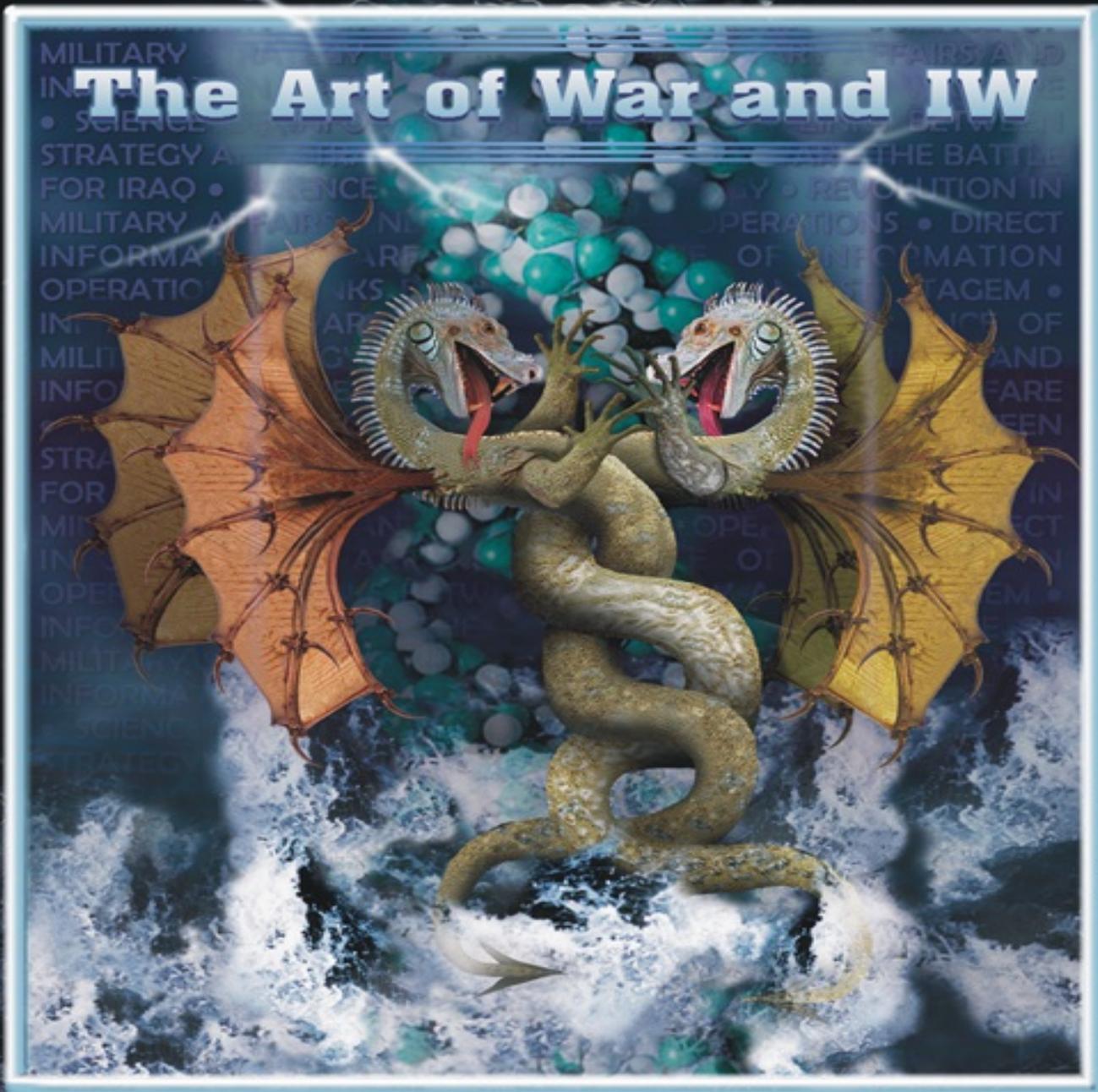


Decoding the Virtual Dragon

Critical Evolutions in the Science and Philosophy of China's Information Operations and Military Strategy



Timothy L. Thomas



Foreign Military Studies Office (FMSO), Fort Leavenworth, KS

Cover

The virtually projected dragons, figuratively depicting the dynamic tensions and electrifying complexities of confrontation between strategy and technology, churn up a stormy ocean of theoretical concepts that stretches across a full spectrum of dimly masked actions and operations. Entwined like strands of DNA, this interlocking and encrypted relationship, coded by the Chinese approach to science and philosophy, shapes methods of engagement and manages their use of information within the multi-layered cultural mix now digitally manipulated and formed by the effects of world views. The vivid image provides an apt metaphor, both for the art of war and for information warfare, which accurately reflects this book's decryptic focus on specific evolutions within the growing thrust and influence of Chinese thought.

Decoding the Virtual Dragon

Timothy L. Thomas

Foreign Military Studies Office
Fort Leavenworth, KS
2007

The views expressed in this document are those of the author and do not reflect the official policy or position of the Department of Defense or the US government.

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 civil-military 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.

FOREWORD

This book expands upon Dragon Bytes, the author's earlier work on Chinese information warfare (IW) activities from 1999-2003. Decoding the Virtual Dragon explains how Chinese IW concepts since 2003 fit into the strategic outlook, practices, and activities of the People's Liberation Army (PLA). The book offers IW explanations directly from the pens of Chinese experts. There are few intermediate filters. In some cases direct translations of key Chinese terms are offered. The Chinese authors discuss the application or relation of IW to strategic thought, the transformation plans of the People's Liberation Army (PLA), the revolution in military affairs (RMA), and the revolution in knowledge warfare and cognition. The book thus serves as a source for the fundamentals of Chinese military thought and demonstrates how IW/IO has been integrated into the art of war and strategy.

China's methodological and thought paradigms with regard to strategic IW issues are quite different from US paradigms. The PLA's science of military strategy, for example, examines basic and applied theory as well as the objective and subjective aspects of strategy. US military strategy, on the other hand, uses a very different set of analytical tools and thought processes. It is more focused on ends, ways, and means or, more recently as US joint publications note, prudent ideas or sets of ideas. Decoding the Virtual Dragon underscores this difference in thought processes and explains how China's strategic approach leads to different applications, methods, and conclusions with regard to IW.

Decoding the Virtual Dragon is designed to update analysts about Chinese IW theory and practice. Of special interest is the Chinese focus on topics scarcely mentioned by US IW specialists such as mobilization exercises, the development of IW countermeasures, the theory of a science of information operations, the holistic and comprehensive approach to strategic issues, and a focus on preemption and IW stratagems.

Both the general military reader and the Chinese security specialist will enjoy this integrated and progressive look at China's IW development over the past several years.

Karl Prinslow
Director, Foreign Military Studies

Office

July 2007

INTRODUCTION

Over the past several years, Chinese information warfare (IW) and information operation (IO) capabilities have become more visible and troubling. These capabilities have been used actively in a series of events aimed at a variety of countries. It is unknown exactly how many Chinese IW reconnaissance or offensive events have transpired or the actual intent of these incursions. Several episodes have leaked into the public domain. Among the most notable are:

- Espionage conducted against the US Department of Defense (DoD) computers, reported in Time magazine. The report concerned a Chinese cyber espionage ring that federal investigators code-named Titan Rain. Its target was DoD computers.[\[1\]](#)
- Chinese attempts to blind a US satellite, reported in Defense News. The report discussed high-powered Chinese laser attacks on a US satellite.[\[2\]](#)
- Chinese hacker attacks on the US Naval War College's net capability, reported in Federal Computer Week. This attack purportedly originated from China and took systems off-line.[\[3\]](#)
- The Chinese destruction of an old Chinese weather satellite with an antisatellite missile, reported on National Public Radio. The report cited a Beijing People's University commentator. He noted that "satellite killing technology is logical in the development of missiles and an IW capability."[\[4\]](#)
- Hacker attacks against Japan or Taiwan, reported in the Japanese and Taiwanese press.[\[5\]](#) The reports noted that these attacks were retaliations for Japan's anti-Chinese interpretations of history and for Taiwanese claims for independence, respectively.

The growing intensity of these IW attacks demands a closer look at China's IW/IO philosophy and how it has evolved. This work attempts to accomplish that goal. Of particular interest is how IW has imbedded itself into the peacetime strategic activities of the People's Liberation Army (PLA) and IW's potential use as a preemptive strategy.

Decoding the Virtual Dragon examines the views of prominent Chinese military theorists on the integration of IW/IO and strategy. It consists of an analysis of seven Chinese books and one Chinese journal article, all focused on information warfare/information operations (IW/IO) related topics. Additionally, a chapter on strategy and information warfare from the author's previous book Dragon Bytes is included. The chapter serves as a link between the old and the new on IW/IO and strategic issues.

The books and article under consideration were chosen for their comprehensive approach and originality in the realm of strategic information warfare theory. Decoding the Virtual Dragon attempts to utilize the expertise of prominent authors to establish a framework behind the PLA's understanding of developments and concepts and their IW application. These developments and concepts include such issues as the revolution in military affairs, war control, preemption, information superiority, and network centric warfare. In many ways Decoding the Virtual Dragon

serves as a one-stop shop for IW/IO concepts and terminology.

The Chinese authors or editors used for this scrutiny are not only some of the most well-known figures within the PLA but also some of the most creative and authoritative. This makes the present work more credible and germane.

Shen Weiguang (Colonel, retired), the father of IW in China, is the author of Deciphering Information Security (Chapter Six) and he was a contributor and editor of the work On the Chinese Approach to the Revolution in Military Affairs (Chapter Three). Dai Qingmin (Major General, retired) authored Direct Information Warfare (Chapter Five) and was the Chief Examiner of the work Study Guide for Information Operations Theory (Chapter Eight). Yao Youzhi and Peng Guangqian, the editors of the work The Science of Military Strategy (Chapter One), are, respectively, the Chief of the Strategic Studies Department at the Academy of Military Science (AMS) and a research fellow of the same department. Both are active duty Major Generals in the PLA. Yao also was the Editor-in-Chief of Warfare Strategy Theory (Chapter Nine). These are just some of the outstanding authors whose works are analyzed herein. In addition, at the end of Chapters Five through Nine, the Tables of Contents of the books under consideration are provided for the reader. This will enable better comprehension of the broad sweep of issues that these authors examined.

However, the reader should also be aware that this volume represents only a very small sampling of the number of books and articles on IW/IO in China. Further, the reader should be aware that the terminology used herein is Chinese and not US terminology. The term “informationization,” for example, is used often. It is another term for the US term “cyberization” according to The Science of Military Strategy. The term “informatized war,” according to the Study Guide for Information Operations Theory, is the Chinese equivalent of “network-centric warfare.” These are only a few of the new terms with which the reader will want to become acquainted.

Not only do the Chinese use different IW vocabulary but they use different definitions, thought processes, and institutions for the study of IW. These issues include:

- A different definition for strategy that examines basic and applied theory as well as the objective and subjective aspects of strategy.
- The use of an Academy of Military Science (an institution that does not exist in the US) to study the science of information operations (an academic discipline that does not exist in the US)
- The use of stratagems to direct packets of electrons
- The development of a University of Information Security
- An updated version of Mao’s People’s War strategy that includes information warfare techniques and procedures
- A focus on developing IW countermeasures (both technical and cognitive) to Western IW strengths
- The frequent practice of information-related mobilization exercises.

Chapter One is an analysis of China’s science of military strategy and thus provides the

context from which to view the other works on IW/IO. The book under examination is a product of the Chinese Academy of Military Science and is titled The Science of Military Strategy. This academy, as does its Moscow counterpart (also called the Academy of Military Science, headed by Russian General Mahkmut Gareev at the time of this writing), offers rigor and an anchor for military (and information-related) thought. The US armed forces lack a similar dedicated think tank (an academy) for military science. The Science of Military Strategy provides a thorough analysis of the basic and applied aspects of the theory of strategy. The Chinese define and understand strategy differently than their US counterparts. The Chinese translated this book into English four years after its Chinese version first appeared in 2001, and the English version is used for this analysis. Three diagrams at the end of the chapter offer this author's understanding of China's military strategy in outline form.

Chapter Two is a review of one article from the journal China Military Science. However, this article is of some importance because Major General Xu Xiaoyan, former Director of the Communications Department (also thought to handle IW issues) of the Chinese General Staff, was its author. The article outlines the military scientific approach to information operations, also known as the science of IO. Instead of the traditional subdivisions of basic and applied theory, the article's author adds a third theoretical subdivision, technical theory. Major General Xu recommends more practical and less theoretical IO activity on the part of the PLA. Perhaps this is why Titan Rain and similar incursions are gaining in popularity in China. An outline of the science of IO is depicted in a diagram at the end of the chapter.

Chapter Three takes a look at selected essays on the revolution in military affairs and the impact of this revolution on strategy and information operations. Several key military authors, to include the authors of the controversial Unrestricted Warfare, wrote essays for this book, titled On the Chinese Approach to the Revolution in Military Affairs. The work offers some key insights into how Chinese strategy will adapt to the demands of the information age. All of the chapter's authors are well-known Chinese analysts of either strategy or information operation topics.

Chapter Four is a reprint of a chapter from this author's previous book Dragon Bytes. The chapter discusses the impact of the information age on strategy. It is included in this volume since it provides background and continuity on the subject matter of IW stratagems. The chapter also allows readers not familiar with Dragon Bytes to know what discussion of strategy, stratagems, and their applicability to IW preceded this work.

Chapter Five presents the thoughts of Dai Qingmin on networks and network warfare from his book Direct Information Warfare. The book is a compendium of definitions and examinations of the various aspects of network warfare. It also includes recommendations on what type of educational process the PLA needs to field a force capable of handling the intricacies of network theory and practice. Dai, former head of the IW Directorate of the Chinese General Staff, points out Chinese interest in two concepts: information supremacy and "integrated network-electronic warfare." This chapter is, for the most part, a summary of Dai's thoughts. The Table of Contents of the book is listed at the end of the chapter.

Chapter Six discusses the important information security work of Shen Weiguang, and is titled Deciphering Information Security. Shen describes a host of information security issues and

lays out an entire program for an Information Security University. Of particular interest to military specialists is Shen's description of the curriculum of the military studies section of the university. The curriculum stresses not only military issues but also economic ones. The Table of Contents of the book is listed at the end of the chapter.

Chapter Seven is a summary of the book An Interpretation of Network Centric Warfare. This book offers a Chinese understanding of the US network-centric warfare (NCW) concept and how the Chinese might adapt to it. The book is divided into twelve chapters. Its discussion and analysis are very detailed and indicative of how closely China studies all US military documents and lessons learned with regard to NCW, to include US military actions in Afghanistan and Iraq. The chapters of greatest interest are those on information superiority and NCW, how to integrate weapons into C4ISR and NCW systems, and battlefield management of NCW. Only the last chapter offers specific comments on China's approach to NCW. The book's Table of Contents is listed at the end of the chapter.

Chapter Eight contains key IW/IO terms from the Study Guide for Information Operations Theory. This book contained 400 IO related questions. For Decoding the Virtual Dragon over a hundred pages of concepts from this work were translated in the identical question-and-answer format found in the original text and then these concepts were summarized/paraphrased for inclusion in this work. The chapter attempts to provide a Chinese understanding of selected IO related concepts in the words of the PLA. Terms such as informatized war, asymmetric war, principles and forms of IW, and other related ideas are discussed and defined. Some questions and answers selected for this chapter focus on how the Chinese view US concepts and policy such as network centric warfare. The Table of Contents is listed at the end of the chapter.

Chapter Nine ends the book in much the way it began—with a look at strategy through the eyes of Yao Youzhi, who served as co-editor of The Science of Military Strategy (2001), the focus of Chapter One in Decoding the Virtual Dragon. In Chapter Nine Yao edits Warfare Strategy Theory (2005). The chapter summarizes the parts of the book that focus on IW/IO and asymmetric warfare. Warfare Strategy Theory has four sections: warfare concepts, features of war, war preparations, and implementation. The Table of Contents is listed at the end of the chapter.

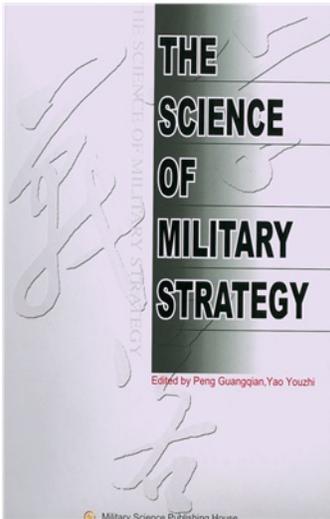
Chapter Ten lists the analytical lessons that one takes from this decoding of the virtual dragon in the cyber age. They are very different from the conclusions that a US audience might take from a similar US study of IW/IO. Naturally, this is because the Chinese are greatly affected by their military science approach to armed conflict, their historical tradition of relying on strategy and stratagems, and their reliance on the dialectic as a way of thought among many other issues.

There are four appendices to the book. Appendix One lists the titles of the articles in China Military Science, the journal of the Chinese Academy of Military Science, that discuss information warfare and related issues from 2004-2006. Appendix Two is a translation of approximately three pages on IW/IO concepts found in the Chinese Military Encyclopedia: information warfare, information warfare technology, and operations research and analysis of information warfare. Appendix Three is a summary of essays on information warfare collected by the author during his attendance at Sun Tzu Art of War conferences in China. Appendix Four is a translation of a key section from the book Forms of Information War by Dong Zifeng. The translation covers the

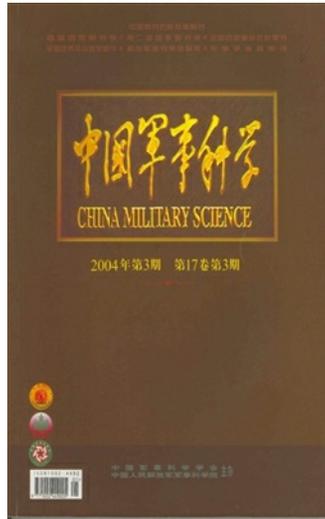
mathematics of computing the strength of combat systems.

On the following pages are photos of the book covers of the works under consideration listed from left to right, top to bottom in accordance with chapter chronology.

Finally, to reiterate, this work serves as an extension to its predecessor, Dragon Bytes. The purpose of Decoding the Virtual Dragon is to look closely at China's IW/IO philosophy and how it has evolved in accordance with the PLA's strategic culture; and to assist analysts as they examine the development of Chinese IW/IO in the near and distant future.



MG Yao, MG Peng, editors, The Science of Military Strategy, 2001



MG (ret.) Xu, "The Science of Information Operations," China Military Science, 2004



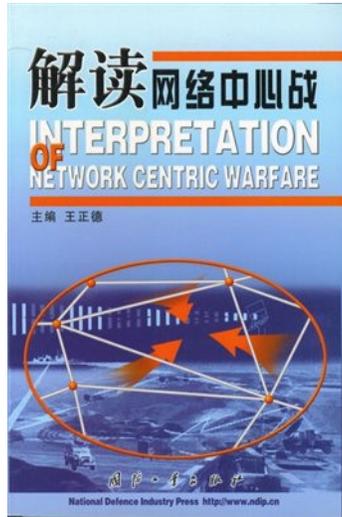
Col (ret.) Shen, editor, On the Chinese Revolution in Military Affairs, 2003



MG (ret.) Dai, Direct Information War, 2002



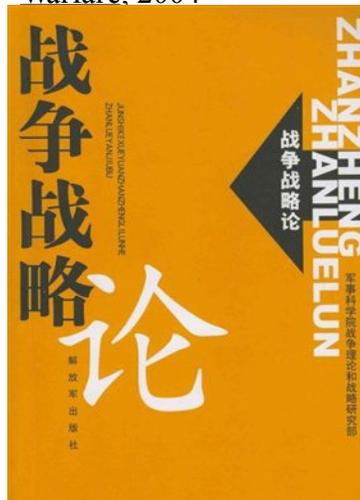
Col (ret.) Shen,
Deciphering Information Security, 2003



Wong Zien Deh, editor,
Interpretation of Network Centric Warfare, 2004



MG (ret.) Dai, Director,
A Study Guide for Information Warfare Theory, 2005



MG Yao, editor, Warfare Strategy Theory, 2005

CHAPTER ONE: THE SCIENCE OF MILITARY STRATEGY

This chapter summarizes [The Science of Military Strategy](#) edited by Peng Guangqian and Yao Youzhi, 2001.[\[6\]](#)

Introduction

How to have our feet firmly planted in China and have the whole world in view, and in the strategic chain of the past, present, and future how to grasp the laws of the evolution of strategic theory and the macro tendency of the development of strategic theory to serve reality, that is the question crucial to the vitality of our strategic studies.[\[7\]](#)

The topic of strategy has long held a central place in Chinese military theory. From the earliest philosophers and tacticians to modern day military pundits, strategy and stratagems[\[8\]](#) have formed a focal point for Chinese military writers. China's ancient scholars, when assessing the character of China's military culture, highlighted a specific military style thinking that "is good at strategy and adept at the use of the indirect method."[\[9\]](#) A recent report on China's military culture noted the following:

... Chinese scholars' way of thinking was essentially a kind of wisdom and war, this lively confrontation between people with all its variables, this arena with all the traits of a game, which provided them with the best stage for giving free rein to their marvelous imaginations and creativity. While it is true that they attached importance to the substance of war, they attached even greater importance to bringing into play the subjective, dynamic roles of people, using strategy to gain victory, and they especially advocated not following one pattern and using the indirect to gain the upper hand.[\[10\]](#)

Sun Tzu and Mao Zedong are probably the two most respected and often quoted Chinese strategic practitioners. There is hardly a bookstore in the US that does not have a copy of Sun Tzu's [Art of War](#) on its shelves. Today even Western businessmen study Chinese strategic methods, to include the 36 stratagems of war, to enhance sales and negotiation techniques.

According to Chinese theorists, stratagems and strategy have witnessed an evolutionary change over the past 30 years, especially in their application. The cause of change was the introduction of information technology and the miniaturization of weapons and equipment. The 1970s and 1980s witnessed the introduction of microtechnologies, advanced missile technologies, the "cyberization" of weaponry (that is, the use of computer chips in weapons for guidance and precision, etc.), and the spread of military technologies into the civilian arena via the Internet. The Chinese also took US forces high-tech experiences in the 1991 Gulf War into strategic account.

Such changes caused Chinese military planners to question the impact of information technology on military strategy and how future wars would be fought. Of key interest was how strategy and technology would be integrated, a question often proposed in articles, books, and

official presentations. In addition to the integration issue, Chinese strategists attempted to keep the “big picture” or long term development of the military in view as another important focal point. Chinese strategists think holistically, having “the whole world in view” as well as the “strategic chain of the past, present, and future” when pondering how to fight future wars.

Two major open source Chinese military works attempted to take these developments and interests under consideration. In 1987, General Gao Rui, a former Vice President at the Academy of Military Science (AMS), China’s premier military think tank, edited a comprehensive open source update of Chinese views on strategy. The manuscript was titled The Science of Military Strategy. It was the first book written and published on strategy in the history of the People’s Liberation Army (PLA). A decade later in 1997, the Chinese military published the Chinese Military Encyclopedia. The encyclopedia’s index contained a comprehensive overview of strategic concepts. For example, the word “strategic” was followed by other terms (pivot, thought, surprise, etc.) seventy-eight times in the index while terms associated with the words strategic or strategy were used twenty-one times. A 2002 addendum to the encyclopedia added another twelve strategy-related items.

However, the pace of change soon overtook not only Gao’s book but also the military encyclopedia’s information. Informationization,^[11] nanotechnologies, economic globalization, the multipolarization of the strategic situation, and the emergence of high-tech local war continued to recast Chinese military thinking on strategic issues. As a result, AMS decided in 2000 to update Gao’s work in a volume under the same title.^[12] The book was published in 2001 with new editors Yao Youzhi and Peng Guangqian. They are, respectively, the Chief of the Strategic Studies Department at AMS and a research fellow of the same department. Both are Major Generals in the PLA and are known for their thoughtful (and sometimes controversial) strategic analysis. Peng, for example, was recently quoted in the Chinese press as stating that the US would not come to Taiwan’s aid in case of a war between Taiwan and China. Yao was identified as President of the China Research Society of Sun Tzu’s Art of War (CRSSTAW). Interestingly, the 2001 book appeared just two years after a 1999 recasting of Chinese rules and regulations (the Chinese equivalent of doctrine). Therefore, the book should offer a look at how new rules and regulations affect strategy.

Peng and Yao’s Science of Military Strategy is an examination of Chinese military strategy from a historical, cultural, and contemporary vantage point. The postscript to the book notes that

The project team tried their best to write a theoretical work which is guided by the Marxist scientific concepts of war and strategy and based on our national and military situation; combines inheritance and development, imitation, and innovation; has the Chinese characteristics and features of the current time; and can play a guiding role in implementing the military strategic guidelines in the new era.^[13]

Work on the volume began in earnest only in July of 2000, so the product represents a fairly quick turnaround.

A well-qualified cadre of professors from China’s Academy of Military Science along with a few other noted scholars helped write the book. Thirty-seven names are listed as contributors

(the book's postscript noted that more than forty people contributed to the work). Twenty-three of the thirty-seven are members of the Academy of Military Science's Department of Strategic Studies, three are members of the AMS Department of Research Guidance, three are from the AMS Department of Military Systems Studies, two are from the AMS Institute of Operations Research, and one is from the AMS Department of Operations and Tactical Studies. Non-AMS participants included one person from the Center for Peace and Development Studies, the vice editor-in-chief of China Military Science, the chief of the editorial board of Military Art Journal, a former chief of Military Science Press, and one person who had no affiliation listed and was listed as just candidate for PhD in Military Science. There is no listing as to who wrote each chapter, however, so Peng and Yao are cited as the editors in all footnotes.

The book has three parts: The Basis of the Science of Strategy; The General Laws of War and the Conduct of War; and High Tech Local War and Strategic Guidance on It. The editors introduce the concept of "science of strategy" (SOS) in the first chapter as well as the SOS's two subdivisions, basic strategy and applied strategy. The book's chapters follow the basic outline of these subdivisions, which the authors establish in the first chapter. Chapters Two through Five of Part One discuss basic strategy. Chapters Six through Nineteen of Part Two discuss applied strategy. Chapters Twenty through Twenty-Four in Part Three discuss how high-tech local war affects the application of strategy. The subdivisions of the SOS give the volume the needed rigor and definitive outline required to cover such an expansive topic. It is important to remember, however, that the book was written before 9/11/2001. As a result this work represents Chinese strategic thinking prior to (and without the hindsight of) the wars in Iraq and Afghanistan.

The discussion below attempts to capture the essence of contemporary Chinese strategic thought as it appeared in the 2001 publication. It is designed to serve as a reference point on Chinese military strategy for the reader, a contextual framework from which to view Chinese IW concepts and their impact on Chinese policy and thinking. IW viewed in isolation offers little of interest. Understanding China's strategic framework is of significant interest as a way to forecast how IW might be employed and which methodologies the PLA might choose.

Peng and Yao devoted one entire chapter of the text to a specific analysis of strategy's relation to information operations/warfare. A summary of this chapter can be found below under the section titled "Strategic Information Operations."

In 2005 the Academy of Military Science published an English version of the 2001 edition of The Science of Military Strategy and this version is used for the summary analysis that follows.

Understanding the Chinese Concept of Strategy

Official Definitions

For purposes of contrasting different ways that strategy is understood, both the US and Chinese military definitions of strategy will be compared. Official US publications, such as Joint Publication 1-02, the Department of Defense Dictionary of Military and Associated Terms, defined strategy until 2006 as "the art and science of developing and employing instruments of national power in a synchronized and integrated fashion to achieve theater, national, and/or multinational objectives."^[14] A shortened version of this definition is just "the art and science of applying

power to achieve objectives.” In September 2006 the term was redefined in JP 1-02 as “a prudent idea or set of ideas for employing instruments of national power in a synchronized and integrated fashion to achieve theater, national, and/or multinational objectives.”[\[15\]](#) Within the umbrella of strategy the JP also defines strategic psychological activities, strategic plan, strategic mission, strategic level of war, strategic concept, and strategic advantage.

The PLA’s Military Encyclopedia defines strategy in the following way:

Strategy is the analytical judgment of such factors as international conditions, hostilities in bilateral politics, military economics, science and technology, and geography as they apply to the preparation and direction of the overall military/war plan. It is advantageous: to study the occurrences and developments in war forecasting/predictions; to formulate strategic policy, strategic principles, and strategic plans; to make warfare preparations; and to put into place directives on the actual principles and methods of warfare.[\[16\]](#)

The PLA’s *The Science of Military Strategy* defines strategy in shorter fashion. First, in a chapter on strategic thinking, strategy is defined as “a general plan to prepare and direct the preparation and implementation of war.”[\[17\]](#) Second, Peng and Yao refer to two Chinese classics that defined strategy. In the 1936 work *Problems of Strategy in China’s Revolutionary War*, Mao Zedong defined strategy as “the study of the laws of a war situation as a whole.”[\[18\]](#) By “war situation as a whole” Mao meant that a war situation requires a comprehensive consideration of its various aspects and stages. The 1997 book *Military Terms of the Chinese People’s Liberation Army* defined the term strategy in the same way as Mao, according to Peng and Yao.[\[19\]](#) Finally, Peng and Yao note that strategy is designed to address the following problem: who takes what means in how large a scope to gain what purpose? This latter understanding of strategy is somewhat similar to a US discussion of strategy by J. Boone Bartholomees, who writes for the US Army War College. He noted that strategy asks questions such as “what is it I want to do? What do I have or what can I reasonably get that might help me do what I want to do? And what is the best way to use what I have to do what I want to do?”[\[20\]](#) Another definition of strategy used at the US Army War College is in broader use. It is attributed to Art Lykke who stated that “strategy = ends + ways + means.” Lykke added that if these three elements were not in balance, then there must be an assumption of greater risk.[\[21\]](#)

Factors Affecting Strategy: Chinese Views

The editors of *The Science of Military Strategy* note that when determining strategy, strategists must take into consideration national interests, war strength, and war potential of opposing forces. They must also consider both international and domestic political situations. International political situations include international political configurations, international coalitions and international organizations, the strategic intentions of major states, and the overall balance of power. Strategists must also consider the influence and restrictions of domestic politics. That is, strategists must take into consideration the nature of state politics (military strategy is determined by politics and military strategy’s aim is subject to that of politics); the classes, nationalities, religions, and interest groups of a state; and the political situation in a state.[\[22\]](#)

Strategy is affected by geo-strategic relationships as well, the editors add. 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 this relationship, 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 relations that may determine the lineups of certain players.[23] Thus, a strategic study must be comprehensive, and it must view war from various aspects and stages (space, time, etc.).[24]

Peng and Yao looked at operations from the aspect of strategy and noted that according to its nature and form, strategy is described as offensive and/or defensive; that the time feature of strategy is either quick decision or protraction; that the space feature of strategy is ground, air, sea, and outer space strategy; that the application feature of strategy is war-fighting and deterrence strategy; and that the major means of strategy are nuclear, conventional, and high-tech.[25] Mao noted that war is a contest in subjective ability between commanders of opposing armies for the initiative and attainment of superiority on the basis of material conditions such as military forces and financial resources. Science and technology, the economy, politics, and military power and potential formulate the objective elements for military strategy.[26]

Factors Affecting Strategy: US Views

The "Guidelines for Strategy Formulation" (found in Appendix One of the US Army War College Guide to National Security Policy and Strategy) are a scientific, creative art that follows certain patterns requiring a common understanding of terminology and adherence to certain principles. Strategy is developed according to time, place, and personalities involved. Enduring values and beliefs are the start point for national purpose, representing the legal, philosophical, and moral basis for the continuation of the American system. Core interests (ends) are physical security, the promotion of values, and economic prosperity. The ways and means to obtain these objectives are based on the national leadership's strategic vision which has ranged from isolationism, global engagement, containment, and primacy. Grand strategic means involve America's national elements of power at the broadest level.[27] The strategist must be able to develop strategies employing all of these elements.

Policy is the start point for strategy formulation at the national level. This involves identifying US interests; level of intensity of each; an evaluation of issues, trends, and challenges; determination of objectives (ends), concepts (ways), and resources (means) to achieve the objectives; feasibility of options; conduct of risk management; and presentation of policy recommendations. The analysis must also identify opportunities and threats to US interests. Strategy formulation at any level employs a strategic thought process based on balancing ends, ways, and means.[28] Strategy should always be end-driven to ensure maximum opportunity to achieve objectives. Each option considered must be examined according to feasibility, acceptability, and suitability, and must be subjected to a risk assessment. The latter is essential to assess consequences if full success is not attained, to include unforeseen second and third order effects.[29]

National security interests are the start point for defining strategic objectives for national

security related strategies. Interests are fundamental concerns of the nation and are written as conditions without verbs, action modifiers, or intended actions. The intensity of interests determines the priority accorded to them, whether they are vital, important, or peripheral. It is important that interests NOT become a function of a threat since this may skew how commitments and resources are allocated.[30]

The Science of Strategy

The focal point for the broader concept of strategy in the 2001 version of The Science of Military Strategy is the term “science of strategy (SOS).” There is no definition in JP 1-02 for the “science of strategy.” The SOS is defined as the military science that studies the laws of war, the laws of the conduct of war, and the laws of the evolution of strategic thought. Its role is to reveal the essence of war and strategy, the various objective elements that influence strategy, and the operating functions and inherent laws that govern strategic thinking activities and strategic “guidance” activities in war.[31] The SOS affects military organization, management, law, mobilization, training, and equipment. It also absorbs the achievements of natural science and other social sciences and disciplines. Peng and Yao note that the SOS is a military science characterized by politics, antagonism, comprehensiveness, stratagem, practice, and prediction.[32]

This last sentence is extremely important because it contains the essence of many Chinese strategic elements discussed over the years. Peng and Yao refer to politics, for example, as the soul of strategy. Antagonism most likely refers to contradiction and the dialectic, or the idea that concepts are always in competition with one another (first there is a thesis, then an anti-thesis, resulting in a synthesis, etc.). The dialectic is a Hegelian concept concerning the process of change in which a concept is converted into its opposite.

Comprehensiveness, the third item in the list, is expressed as a comparison of either certain factors in international relations or various Chinese internal factors. The term “comprehensive” is an all-inclusive method for examining a state’s power base. It is different from the old Soviet term meaning correlation of forces in that it is a more holistic consideration of the impact of many issues on strategy and power: the economy, culture, the military, and other such issues. Examples of Peng and Yao’s use of the term “comprehensive” in their book include the following:

- Comprehensive national power (CNP)
- Comprehensive sea power (CSP)
- Comprehensive strategic interest (CSI)
- Comprehensive strategic targets (CST)
- Comprehensive strategic benefits (CSB)
- Comprehensive cyberized war (CCW)
- Comprehensive confrontation capacity (CCC)
- Comprehensive national defense construction (CNDC)
- Comprehensive support efficiency (CSuE)
- And comprehensive national strategy (CNS).

The term comprehensive national power is calculated year by year by specific institutes in China based on select criteria.

The concept of stratagems is perhaps the most important characteristic of the SOS since it represents the methodology of expressing strategy in practical terms. According to the records of the Han Dynasty, ancient Chinese military strategists were classified according to one of four groups: power and stratagem, disposition and capability, Yin and Yang, and technique and skill. [33] The purpose of the group known as power and stratagem was “to defend the state by orthodox methods and to use force by unorthodox methods” with the latter sounding quite similar to the US concept of asymmetric war. Modern day Chinese strategists are closest to the power and stratagem group according to Peng and Yao. They note that the SOS is “a science of wisdom to sum up the laws of using stratagems.” [34] Peng and Yao add that Caesar thought stratagem was more important than arms, and that Lenin said there cannot be war without stratagems. Western strategic theories, the editors note, appear to be more disordered and not very systematic in comparison with China’s strategic abstraction and generalization. [35]

Finally, the editors note that practice and prediction are also characteristics of the SOS. Practice means that strategy is not simply based on pure thinking. The science of strategy rests with practice. [36] However this may be the weakest link in the PLA’s theory of strategy. They have not “practiced” much in the past 50 years other than in local exercises. Prediction is not based on simple analogy or inference but rather from a deep analysis of all relevant elements and intentions based on a full and complete understanding of the objective conditions. [37] Again, Chinese theorists may not be able to predict as well as they might expect due to a lack of practice.

The SOS is very precise and detailed. It has two classes or subdivisions: basic strategic theory and applied strategic theory. The next two sections of this chapter, devoted to these issues, are short summaries of the important points of each. These summaries are paraphrases of key issues intended to allow the reader to attain for her or himself a Chinese view on each issue.

A detailed outline of the science of strategy is located at Diagrams 1A-1C at the end of this chapter. These diagrams are the result of this author outlining Peng and Yao’s final discussion of the theoretical system of the science of strategy. The diagrams are unique for their visualization of the elements of strategy from a Chinese perspective, a dissection not familiar to US audiences. [38]

Basic Theory of Strategy: Basis of the Science of Strategy

General: Primary Divisions of Strategy’s Basic Theory

The Chinese military subdivides the basic theory of strategy as follows:

- Concept of Strategy (the relationship between war and strategy, targets and categories of SOS studies, scientific connotations of strategy, status of SOS in military art, strategic elements, strategic classifications, and stratified structure)
- Related Elements of Strategy (politics, economy, science and technology, national interests, geography, cultural tradition, military force)
- Development History and Evolutionary Laws of Strategic Theory (study of historical paths leading toward the development of strategic theory)
- Essence and Laws of Strategic Thinking (considers strategic thinking as the top level)

of military art based on the dialectic)

- Methods of Science of Strategy Studies (scientific theories of knowledge and methodology in the strategic field. They orient, process, and examine strategy and look at the integration of abstraction, logic, systems, and Marxism and case studies).

Concept of Strategy

Peng and Yao note that there are strategic concepts called the determinants of strategy. However, before listing these, the editors made the following statement that gives 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' personally 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 having a bearing on war strategy and reveal their inherent connections with war strategy.[\[39\]](#)

Many of the primary characteristics of the Chinese concept of strategy shine through in this quote. First, Chinese strategists look at objective conditions such 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. They then use creativity and stratagems (subjective guidance) to manipulate these objective factors to their benefit. 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 when force will be used and when diplomacy will be used).

Related Elements of Strategy

Even though strategy is determined by the application of subjective guidance to the objective conditions before it, there are other determinants as well. The editors list seven elements of strategy—politics, economy, science and technology, geography, cultural tradition, military force, and national interest. The latter element is the most important. It is both the starting point and destination of military strategy according to the editors.[\[40\]](#)

The editors define national interest as the first determinant of strategy. It is an aggregate of objectively physical and spiritual requirements of a state whose existence and development depend on such interests being protected. Spheres of national activities can be divided into national political interest, national economic interest, national military interest, and so on. Generally speaking, national interests involve national territory, security, sovereignty, development, stability, and dignity.[\[41\]](#)

War strength and war potential are a second determinant of strategy. Both elements help determine the material base for strategic planning, are the fundamental means to win wars and secure military strategic objectives, are the means to contain and restrict war, and are the most active elements in the ability to change military strategy.[\[42\]](#) A third determinant is the geo-

strategic relationship. This includes the components of the geo-strategic relationship, such as geographic position, size and shape of territory, natural resources, the national capital's location, frontiers and national boundaries, relative distance between states, and grand strategic space (maritime, atmospheric, and outer space).[\[43\]](#)

Another determinant of extreme importance is culture. The editors define culture as “the sum total of a state or a nation's spiritual and material precipitations accumulated under a long-period of influence of its natural circumstances, social pattern, and economic level.”[\[44\]](#) Strategic thought is always formed on the basis of certain historical and national cultural traditions, and the formulations and performance of strategy are always controlled and driven by a certain cultural ideology and historical cultural complex.[\[45\]](#) Different cultures bring various understandings of our world to the table. The significance of strategic culture, the editors note, primarily lies in providing a fundamental paradigm for decision makers to cognize and judge the strategic environment.

China has developed the concepts of peaceful coexistence and a virtuous interaction between states as its model while Western mainstream culture, Peng and Yao believe, stresses a struggle for existence (Darwinist) or the law of the jungle.[\[46\]](#) Conflict-oriented strategy still holds a strong place in Western strategic culture. Expansion and the seizure of hegemony are Western strategic targets while China's has been an introvert-type behavior whose targets are peace, safeguarding national territories, and seeking unification and resisting aggression.[\[47\]](#) Clearly, Yao, Peng, and the other contributors to this *The Science of Military Strategy* view Chinese intentions and their interpretation of Western strategic culture differently than do many in the West!

Further, with regard to culture (and indirectly to the issue of Taiwan) it was noted that

The cultural history of the Chinese nation lasted more than 5000 years without interruption, forming a national cultural tradition with its unique characteristics. The benevolence and self-discipline of the Confucius school, the slight to force and indifference to fame and fortune of the Taoist school, the diligence and sincerity of the Mohist school, the tactics and stratagem of military science, the sizing up of situations of political strategists and the education on farming and warfare of legalists all had tremendous influence on Chinese strategic thinking and strategic culture. Chinese philosophy values identity and unification. Chinese history is a history of a unified multi-national state for more than 2000 years. All these imprint firmly and deeply the idea of unification on the psychology of the nation.[\[48\]](#)

A final determinant of strategy is international law. It is a code of conduct having a legally binding force on every state in international relations. Subcomponents of international law include systems and fundamental principles, influences and restrictions, and the relativity and limited validity of international law. This latter point implies the Chinese envision a degree of flexibility in their interpretation and use of international law.

History and the Evolution of the Laws of Strategic Theory

An important subdivision of the basic theory of strategy is the evolution of the laws of strategic theory. The editors highlight Marxist theory as the forerunner of a revolution in strategic

theory, and PLA writers today and in the future are expected to continue to stress the importance of Marxism. Peng and Yao note that

The scientific world outlook of Marxism, like an illuminating light, brightens military science, founding military strategic theories on the scientific base of historical materialism, so it becomes a science in a real sense. Marx's principle on People's War and his strategic thought of active defense and concentration of forces are of epoch-making significance in the history of the development of strategy.[49]

The historical influence of Marxism cannot be overestimated. In 1849, Peng and Yao note, it was Engels who suggested the People's War concept. That is, Engels and not Mao is the father of the concept of People's War. Both Marx and Engels held that the most effective defense is active defense, where one can influence the enemy by defensive actions and thereby not be controlled by the enemy.[50] Mao Zedong's military strategic theory is the practical application and specific reflection of Marxist military theory in the Chinese revolutionary war. "Mao Zedong's military strategic theory is a China-styled Marxist military strategic theory," the editors note.[51] The editors state that the main parts of Mao's Marxist view of strategy shows that the law directing war as a whole reflects an essential relationship among component parts and factors of the entire war. [52] Mao's main role is serving as the integrator of thoughts.

According to Peng and Yao it is the political objective that forms the fundamental basis of military strategy. Political mobilization and political programs are the "soul of military strategy." Strategy must be formulated with the characteristics and development of war in general taken into consideration. Each war (revolutionary war, general war, etc.) has its own specific laws.

Finally the implementation of strategy is a contest between the subjective ability of commanders of both sides to direct the war.[53] Mao noted that war is a contest in subjective ability between commanders of opposing armies for the initiative and superiority on the basis of material conditions such as military forces and financial resources.[54]

Laws of Strategic Thinking

The laws of strategic thinking are another subdivision of the basic theory of strategy. Strategic thinking formulates, according to strategic factors, strategic thought, strategic guidelines, and strategic decisions. Strategic thinking is the specific manifestation of thinking at the top level of military art and the specific application of epistemology and methodology in military arenas. [55] All modes of thinking such as logic-thinking, image-thinking and inspiration-thinking can theoretically raise the quality of strategic thinking. These modes reflect practice and are the specific processes of thinking by the strategic conductor.[56] The characteristics of strategic thinking that Peng and Yao describe include:

- Totality (comprehensive look at the parts and elements)
- Confrontation (contest of material and spiritual forces)
- Certainty (start with the fact that war is full of uncertainty about the enemy situation but end with certain conclusions about the enemy)
- Foresight (use history, current factors, wisdom, and resolution to visualize future war)

- Creativity (the soul of strategic thinking requires subjective initiative to surpass experience and tradition)
- And inheritance (culture).[\[57\]](#)

Peng and Yao listed five models of strategic thinking. Objective and subjective thinking is one model. Objective strategic thinking refers to thinking activities which, taking war as a start point, reflect the objective laws of war and strategy. Subjective strategic thinking refers to thinking activities that make strategic judgments and decisions based on subjective will, especially the data and experience in one's mind. Closed and open strategic thinking is a second model. Closed strategic thinking relies on experience and tradition and does not make or rely on information exchanges with the outside world. Open strategic thinking means models that exchange information with the outside world and are good at substituting old thinking methods with methods full of vigor and adaptability.[\[58\]](#)

A third model of strategic thinking is the stratagem type and force type, divided according to the application of strength (soft stratagem or hard force) applied by the strategic subject. Winning by stratagem has always “been the main idea of traditional Chinese strategic thinking. It means the use of limited force to achieve victory or to realize the aim of the war.” Western thinking, according to Peng and Yao, pays more attention to contests of strength, emphasizing direct confrontation or force type models.[\[59\]](#) Two final models are conservative versus creative strategic thinking; and unitary versus systematic strategic thinking.[\[60\]](#)

The laws of strategic thinking according to Peng and Yao also include “ways” that strategic thinkers direct wars in order to understand the problems of war as a whole. Also called methods, these “ways” include the following:

- Macro operations (know the situation as a whole)
- Historical deductive methods (discover general laws, apply them under new conditions)
- Methods of system integration (introduce the achievement of system science into the process of strategic thinking, examine and view wars as a total unit)
- Methods of mathematical reasoning (rely on quantitative analysis, the collection, collation, computation, and analysis of data using numerical value as a measuring criterion)
- Methods of dynamic tracking (how a subject dynamically understands the situation by following flows of personnel, material, and information—studying the fluidity of war to understand its development and feel its pulse)
- Methods of stratagem confrontation (thinkers must confront the enemy through deducing the war in his/her mind and directing strategic activities with better wisdom—analyze truth and falseness, compare strength and weakness, and employ orthodox and unorthodox tactics via dialectics. A stratagem is made up of dialectics, logic, math, and other scientific methods)
- Methods of prediction (make correct inferences or judgments based on knowledge of the objective laws of war)
- And methods of experiment and simulation.[\[61\]](#)

Chinese Methods of Strategic Studies

Strategic studies are cognitive activities in the sphere of strategy, a process to raise, analyze, and solve strategic problems. The Chinese believe that Marxist methods provide a golden key to analyze strategic problems comprehensively, dialectically, objectively, systematically, continuously, concretely, and connectedly.^[62] Just and unjust wars fall under this category of methods as well. Just wars facilitate the progress of society and promote the liberation of productive forces, such as People's War, revolutionary, and anti-aggressive war. Wars are unjust if they hinder society's progress and strangle new productive forces.

General methods of scientific study are cognitive methods and include specific applications of the Marxist philosophical method. Frequently used methods in strategic studies, which differ little from US methods, are the inductive (method of inference from individual to general), deductive (deduce from general to individual), analogy (inference from similarity between two things to that of two other things), and mathematical (judge the development of something from its quantity). Specific methods of scientific study, on the other hand, include:

- Systematic analysis (view war as a whole by taking mutual relations and the influence of exterior environments into consideration)
- Statistical analysis (collect data and then calculate or categorize according to qualitative definitions to express quantity in the form of figures)
- Comparative study (philosophical, historical, political, strategic, and cultural viewed in time, space, and qualitative and quantitative comparison)
- Cause and effect analysis (for example, finding the relation between history and reality from a dialectical materialist interpretation of events)
- And social investigation (using sample or model investigations).^[63]

Chinese specific study methods also deal with case studies. They include the study of selected battles, war simulations, live operational demonstrations, and the synthetic analysis of military situations (which sums up all military intelligence and strategic information gathered from various sources to determine their inherent relation).^[64]

Applied Theory: General Laws of War and the Conduct of War

General: Primary Divisions of Strategy's Applied Theory

The second subdivision of the Science of Strategy (SOS) is applied theory. Applied theory is the practical system that studies the laws of strategic guidance. It consists of two parts, strategic formulation and strategic performance. These two parts are further subdivided as follows:

Applied Theory of Strategy

1. Strategic Formulation
 - a. Strategic Judgment (nature of a threat, posture, intention)
 - b. Strategic Decision making (strategic aim, mission, guidelines, and deployment)
 - c. Strategic Planning (pre-arrangements for war)

2. Strategic Performance
 - a. Strategic Guidance for the Construction of Military Force
 - b. Strategic Guidance for the Employment of Military Force (operations such as strategic command; strategic maneuver, strategic offense and strategic defense; strategic air raid and anti-air raid; strategic IW; strategic psychological warfare; and strategic support. Developing laws for high-tech local wars is a new field in this subset) [65]

Only one subset of strategic formulation (strategic planning) and one subset of strategic performance (strategic guidance for the employment of military force) will be covered below. Short summaries are presented of each.

Strategic Planning: Subset of Strategic Formulation

Strategic planning is of particular interest. Peng and Yao note that the task of strategic planning is to restrict war, make war preparations, and win victory in war, in that order. [66] A wise strategist's first step is to soberly estimate the war strength and potential of an opposing force in order to analyze the basis of war. [67] Intimidation, efficient war power, limited deterrence means, and some form of parity are the best ways to contain and restrict war. [68] There are three elements to carry out a deterrence strategy: appropriate military strength, resolve, and the will to use force. It is necessary to persuade an opponent to perceive such strength and resolve. Deterrence strategy can be subdivided as follows: according to purpose and nature into offense and defense; according to degree into superiority, parity, limited, and minimum; according to scope into overall and partial; and according to structure into conventional, nuclear and bio-chemical weapons. [69] War preparations should be underway even in peacetime in case strategies to contain and restrict war fall short.

Strategic Guidance for the Employment of Military Force: Subset of Strategic Performance

This section offers short summaries (usually one or two paragraphs) of chapters 6-19; and a short summary of Part Three ("High-Tech Local War and Strategic Guidance on It") of The Science of Military Strategy. The titles of each chapter are listed in *italics* at the start of each section. The purpose of these summaries is to highlight for the reader the various elements of Chinese strategic thought. Again, all of the following sections are elements of the applied theory subdivision of the science of strategy; and all of the summaries are based on Peng and Yao's PLA definitions and discussions.

Strategic Information Operations (IO) and Strategic Psychological Warfare (SPW)

This first summary is a combination of two chapters (*Strategic Information Operations; and Wartime Political Work and Strategic Psychological Warfare*). It is longer than the other summaries since IW/IO is the prime focus of Decoding the Virtual Dragon.

Peng and Yao define *strategic information operations* as strategic actions that employ information weapons to influence the enemy's information and information systems while

simultaneously protecting one's own information and information systems so as to gain "information superiority" on the battlefield. The term information weapon indicates that the cyberization of weapon systems have supplemented traditional weapons.[70] An information weapon is a term not in current use in the US lexicon.

The editors note that the use of information weapons and other information related products has raised information operations from the operational and tactical level to the strategic level. IO now can guarantee the seizure of the initiative in war where a major pattern of operations has become information confrontation. The outcome of a war now depends in part on another term unfamiliar to Western audiences, information control.[71]

Strategic information operations have specific characteristics according to Peng and Yao. One characteristic is that the level or degree of cyberized weapons can decide a country's war strength, and thus the seizure of information has become a primary task of modern warfare. A second characteristic is that small-scale tactical operations can sometimes achieve strategic results owing to the fact that geographical distance has lost much of its traditional significance in the information age. A third characteristic is that targets have changed. In traditional warfare, targets were the enemy's weapons and equipment. Now targets include intelligence, reconnaissance, communication, and command and control systems which make information systems and decision making processes important targets in every phase of a war. Finally, IO is an important element of any holistic or comprehensive strategic operation. This increases battle space (where information and cyberized processes work) and reduces force density since fewer people are needed on the battlefield.[72]

Peng and Yao list five types of strategic information operations. They are:

- Intelligence warfare. It provides support for making decisions, and it can be divided into intelligence reconnaissance (space, network, etc.) and intelligence protection (information security)
- Command and control warfare. This includes the use of various means to attack an enemy's command and control element and destroy his information flow. This is the primary task of IO whose essence is to capture the battlefield initiative
- Electronic warfare. Its purpose is to seize electromagnetic command on the battlefield. Attack, defend, and support are three types. Space electronic warfare is a potential future method
- Cyber warfare. It consists of soft kill (damage or destroy computers and networks) options and is a new operational pattern consisting of attack and protection
- Destructive warfare of information sources. It consists of hard kill (precision-strike cyberized weapons that destroy C4ISR and other relevant systems) options.[73]

Finally, Peng and Yao stress the importance of strategic guidance when implementing strategic information operations. They note that information superiority and information dominance must be maintained in order to keep the battlefield initiative and bring the power of information systems and cyberized weapons to bear. Operations must remain integrated to defeat an opponent in a system-to-system confrontation.[74] Further, war preparations must be made ahead of time (to include the recruitment of information talent) to ensure that an IO can be conducted suddenly with

the use of all civil-military links.[75]

However, the most important idea regarding strategic guidance, and one of the most important ideas for Peng and Yao's book in general, is that IO is directly linked to the gain or loss of the initiative in war and thus "priority should be given to the attack and combining the attack with the defense." Launching preemptive attacks to gain the initiative includes "striking the enemy's information center of gravity and weakening the combat efficiency of his information systems and cyberized weapons." [76] This allows one to weaken the enemy's information superiority and reduce his holistic combat efficiency. [77] One can only guess if the Titan Rain incursions and other similar events were designed to recon Western information systems and prepare the way to strike these information centers of gravity in time of conflict or leading up to conflict.

In addition to the book's chapter on strategic information operations, the text of The Science of Military Strategy is spotted with references to information operations throughout that add additional points of interest to the discussion. In most cases the discussion is very different from that encountered in the strategic information operations chapter recounted above.

One such discussion covered information control. Peng and Yao noted that the essence of IO is to use information flows to control the energy and substance flow on the battlefield and thereby seize the command of battlefield information. It is important to seize information control, they add, because it will become the prerequisite for seizing the command of air, sea, and land in future battles. [78] Weapon platforms, command, control, intelligence, communications, and logistics are integrated into operational systems. Integrated systems offer a new field in which to play. One who controls the information process can seize the strategic initiative or deliver precise, paralyzing strikes. [79] One writer not associated with Peng and Yao's work has even suggested that control be considered a new form of war along with offense and defense. [80]

It is clear that as acquisition, awareness, transmission, and control of information becomes more and more important in modern wars, the establishment of a full dimensional, long-range and multilayer space detectable, strategic reconnaissance system is of great value. A highly responsive, reliable, smooth command, communication, and intelligence system can be of decisive significance in winning the initiative in war. [81]

Peng and Yao stated that defense science and technology efforts provide the key indicators for the development of IW/IO. Chinese scientists must develop modern weapons and equipment, particularly "trump card" weapon systems that enhance strategic operational capabilities. [82] Commanders must employ operations research, systems theory, and information theory in order to make profound qualitative and quantitative analysis of battlefield actions. [83] Battlefield construction should be directed against an enemy's reconnaissance. This means that concealment and camouflage techniques need to include antioptical, anti-infrared, and antiradar reconnaissance devices. [84]

The editors also discussed the impact of information weapons on society as a whole and on military art in particular. First, since IW offers a more powerful soft destructive force, the line between peacetime law and wartime law is more blurred according to the editors. Laws must be

created to reduce the potential destructiveness of high-tech warfare.[85] Second, high-tech war, especially informationized warfare, involves all sides of social life, and the entire society of China must be mobilized to fight such a war. Scientific and technological mobilization involves high-tech workers, those with high academic degrees and expertise in scientific research institutions, universities, colleges, and high-tech corporations. These individuals, once mobilized, will be enrolled in the reserve forces.[86] This indicates that, with more science and technology in weapons and equipment, knowledge will become the dominant factor of combat power, and the contest eventually will be between highly qualified personnel.[87]

Third, peacetime IW/IO requires standardized laws, regulations, and statutes for various aspects of the military field.[88] The initial battles are usually of a determined nature and the period of transition from peacetime to wartime can be quite short in the informationized age. A national political system that can integrate national economic construction with war preparations must be developed.[89] This development may mean an enhanced role for information deterrence, deterrence that depends on the powerful performance of information science and information technology when put into effect by the momentum and power of information warfare. Information deterrence's features are "permeability, replaceability, transmissibility, diffusibility, shareability, predictability, ambiguousness, two-way containment, People's War, and diversity." [90]

Fourth, with regard to military art, the information age has brought about the advent of the concept of information warfare strategy. This is a new concept and type of strategy, according to the editors. Its goal is to seize and maintain strategic information superiority and battlefield information superiority and secure strategic objectives through information control and information attack that includes both soft damage and hard destruction. This, of course, includes cyber attacks on the infrastructure and information resources or systems on which a country's armed forces depend.[91] Here one is reminded of the recent Chinese reconnaissance activities at the US Naval War College. Struggles in the field of information between opposing sides will lead to changes in the form of strategic maneuver as well. Maneuver of a strategic information operations force may become a new form of strategic maneuver in future wars.[92]

Information has gradually become a force multiplier in the opinion of Peng and Yao, and the modes and means of strategic support enhance the collection, transmission, and utilization of information.[93] Strategic operational support's emphasis will be on countermeasures based on information systems and information technology in such fields as counter-reconnaissance and the safety of an information network.[94] For example, an air attack in the absence of IW and EW support results in an 8-10% chance of being shot down, while with IW and EW chances of being shot down plummet to .03%.[95] Thus it is clear why the "three abilities" needed for air defense systems are cyber attack, cyber defense, and information handling ability, which is the collection, transfer, processing, and storage of information. EW is also a major task for the command and control of strategic air defense in modern times.[96]

Psychological operations are a component part of information operations in both China and the US. Peng and Yao's book included a chapter on "*Wartime Political Work and Strategic Psychological Warfare*." [97] Of the two topics, strategic psychological warfare (SPW) is more relevant and useful since most Western organizations do not have political officers. SPW is defined as strategic confrontational actions in which psychological offensives are launched

according to psychological principles to undermine the morale of enemy troops and civilians or to eliminate the consequences of an enemy force's deceptive propaganda. It is a component part of wartime political work.[\[98\]](#)

SPW is conducted in both peacetime and wartime. Peng and Yao write that the West has promoted psychological warfare in peacetime in many ways. These include attempts to advance their political system and life style, to use economic aid as bait, to seek economic infiltration and control, and to promote western values via radio, TV, movies, newspapers and journals, audio and video products, and especially over the Internet.[\[99\]](#) Modern psychological war, Peng and Yao add, is getting more integrated into society but is often concealed. They list five methods of concealment. First is the news, where psychological influence is often accepted by people without their realizing what is happening to them. Second is the way culture and art exchanges permeate psychological warfare's content. Third are academic activities which also exercise psychological influence. Fourth is the conduct of psychological warfare via unofficial people-to-people exchanges. Finally there are special psychological warfare activities conducted by special service agencies.[\[100\]](#)

The editors also note many military uses of SPW in wartime. They state that the primary target of strategic psychological warfare is enemy strategic decision makers. The purpose of SPW is to cause them to make mistakes in perception, judgment, and decision making and thereby enable one to subdue the enemy without fighting. Today military objectives are more closely integrated with political and psychological objectives than in the past primarily due to the information factor. Military strength, however, remains as the material basis of psychological warfare whether it is for deterrent value or for precision strike value.[\[101\]](#)

Modern science has provided new military means of psychological warfare. The future conduct of battlefield propaganda will be by smart unmanned aerial vehicles (UAVs) and leaflets that have both audio and visual functions. Information denial will be used to cause psychological vacuums, tension, and confusion; computer viruses will be used to make computer operators psychologically perplexed; and false information will be implanted into command and control systems to cause psychological misconceptions when utilizing these systems.[\[102\]](#)

Peng and Yao note in conclusion that China's objective requirements to ensure that the PLA will gain the strategic initiative in future high-tech wars will require:

- Acting from the demands of high-tech wars and the international psychological struggle
- Exploring effective ways to strengthen the PLA's psychological warfare force
- And developing a complete set of psychological warfare tactics and methods with PLA characteristics.[\[103\]](#)

Wartime political work, the other part of the chapter on psychological warfare, refers to the ideological and organizational work of the armed forces while performing combat tasks. Such work can dispel any negative political or spiritual factors in the force while also magnifying any factors in the enemy camp that are to the PLA's advantage. Wartime political work is an important guarantee, from the Chinese perspective, of the following factors:

- Realizing the Chinese Communist Party’s leadership over military operations
- Conducting People’s War under modern conditions
- Bringing into play the efficacy of weapons and equipment
- Bringing into play the human factor and making up for a deficiency in weapons and equipment (to include the use of the subjective initiative)
- Improving and maintaining joint operational capabilities
- And sustaining the troops fighting capabilities and accomplishing combat tasks.[\[104\]](#)

Basic tasks in wartime were also listed. These included the following:

1. Carry out mobilization and propaganda before, during, and after combat
2. Adjust and strengthen organizations in a timely manner to ensure the uninterrupted and effective filling of vacancies caused by combat
3. Promote military democracy, which is relying on the masses to provide wisdom
4. Publicize heroic deeds and spread the news of victories
5. Maintain battlefield discipline
6. Fight against an enemy’s psychological warfare capability and incite defection
7. Annihilate enemy forces but treat prisoners of war leniently
8. Carry out political work on militias and laborers to get them to join the battle
9. Take care of the wounded and disabled
10. Perform ideological work on military dependents and those working in the rear.[\[105\]](#)

Finally, there were three other lessons for the conduct of psychological warfare in the information age. First, the collection, analysis, storage, and transmission and processing of battlefield information was deemed very important. These missions keep one up to date on recent changes and enable the conduct of effective psychological warfare. It is more important than ever to respond promptly to change in the information age. Second, mobilization activities should be continuously held. The reason again is that change is so rapid that emergency measures only implemented in wartime will lead “to being at a loss at a critical moment.” Third, it is now apparent that quality counts more than numbers and that wisdom and skill count more than physical stamina and courage.[\[106\]](#)

Local War under High-Tech Conditions

Emphasis should be unswervingly placed on preparation for two successive operational tasks in two strategic directions, that is to say, carrying out decisive operations in the main strategic direction and carrying out preventive and controllable strategic operations in the other strategic direction at the same time.[\[107\]](#)

This summary, which also has IW/IO overtones, is Part Three of The Science of Military Strategy. Part Three is titled “High-Tech Local War and Strategic Guidance on It.” This concept is considered as a new addition to Chinese strategic theory, and is denoted in the diagram of the science of strategy at the end of this chapter as a dotted line in the applied theory diagram.

Peng and Yao started the section with a description of the new international environment in

which China must operate. Competition, they note, has moved from a bipolar pattern to competition involving comprehensive national power (CNP). War is now more controllable, smaller in scope and size, and efficient. Strategic powers are now more mutually dependent and restrained.[\[108\]](#) There is concurrent emphasis on both deterrence and war-fighting. Political objectives are limited, force utilization is more integrated, operational means are based on information, and more stress is placed on comprehensive strategic interests (CSI) than on war's destructive power.[\[109\]](#)

China will not ally with any big power or group of states.[\[110\]](#) China might face two types of local wars: outside aggression and invasion, or a fight over reunification. Wars for China will remain defensive in nature and just. Wars will be fought on China's strategic front lines and not deep inside the country which is disadvantageous to China. This is because the battlefield is limited for maneuver, the natural environment will affect operations, and border areas are the real centers of conflict of nationalities and religions. Threats may come from multiple directions.[\[111\]](#) China has to fight a People's War under modern conditions with regard to war preparations and implementation. As a result, unity of the masses remains vital.[\[112\]](#)

The editors then describe high-tech war. They state that it is continuous and of high-tempo, reflecting the rational control of war based on unprecedented military capability.[\[113\]](#) The twenty-first century has brought information age developments, economic globalization, multipolarization in world politics, and militaries armed with advanced technology. Those with advanced technologies possess militaries that can impose their will on others.[\[114\]](#)

To win in high-tech local war, China must not be intimidated, and it must always seek to maintain the initiative. It must never fight at a time and place the enemy expects, and never fight in a style that the enemy anticipates. It must attack an enemy's weak points with China's strong points.[\[115\]](#) The definition of asymmetry is not only limited to combat forces but also covers operational domains, weaponry, operational modes, and methods. These means are used to gain the initiative, reduce loss, and defeat the enemy quickly. A weak side in a conflict may employ stratagems to change operational methods and thereby reduce loss and gain victory.[\[116\]](#) These are old methods that can utilize new high-tech means to employ forces in ways never before imagined.

A People's War philosophy will still be relevant and can help with preparing the country both materially and spiritually for battle. One must mobilize, organize, and arm the masses according to the requirements of high-tech local war.[\[117\]](#) Rapid mobilization based on prior preparation is the key. It is also necessary to create new People's War strategies and tactics to give full play to China's CNP; to combine high-tech weapons with low-tech weapons; and to combine military warfare with political and economic warfare.[\[118\]](#) Defense is based on deterring war while preparing for war in peacetime and on the unity of a strategic defense combined with operational offense and defense in wartime.[\[119\]](#) Since there is little or no difference between the initial and subsequent phases of battle, tactical and operational battles can have strategic significance. China must stress conducting active strategic counterattacks on exterior lines to achieve the aims of strategic defense.[\[120\]](#)

China's specific understanding of the characteristics of local war and its context is not terribly extensive due to a lack of experience in the area, but interesting nonetheless. First, China's

military strategists look at war space as the objective environment in which a war is prepared and implemented. This environment is divided into direct combat space of offensive and defensive operations and space indirectly related to the implementation of war. Today direct combat space is reduced and related war space has increased (put another way, operational space is reduced and strategic space has increased).^[121] Operational space is reduced since (1) there are limited political aims today (2) interests are now more integrated (3) the morality and justice of war plans are of greater importance and (4) the risks and costs of a war's expansion restrain war.^[122] Now it is easy to obtain the objective of war through one campaign or one battle.

Second, the steps in a high-tech local war are: crisis development, international mediation, confrontation intensification, outbreak of war, peace negotiations, and peacekeeping activities. The idea of sudden attack has changed. It doesn't mean "surprise" but rather that one side can't correspondingly react even though the situation is known due to one side possessing high-tech and the other only low-tech means. Preparation and mobilization are more important than ever before.^[123] One has to know how to seize the initiative first and take calculated risks to win in high-tech war.^[124] The subtlety of strategy lies in the concentration of strength^[125] which allows for good risk taking.

Third, victory depends on the comprehensive confrontation capacity (CCC) of the whole combat system. Systems confrontation and one's overall strike potential is more important than the concept of independent operations.^[126]

Fourth, a new war pattern of "strategic decision making--operational command--tactical action" has come into being. Weak sides should make good strategic preparations and organize to take quick actions against an enemy. Full play must be given to human subjective initiatives and using cost cutting measures to counteract the technology gap.^[127] The inferior side should give full play to its subjective initiative.^[128] Concentration in time is more important than concentration in terms of space.^[129]

Finally, future military operations will include preventive strategic actions or operations (deterrence operations such as rehearsals, alerts, no-fly zones, etc.), controllable operations (restore and stabilize a situation where a war crisis has appeared—includes air attacks, island attacks and defense, frontier counterattack, and medium- to large- scale joint ops in special situations), and decisive operations (medium-large scale high-intensity operations next to general war).^[130] No agreements can be reached in negotiations without a display of adequate strength and determination. Fundamental interests can never be compromised.^[131]

Short Summaries of Other Chapters

Listed below are summaries of other chapters of *The Science of Military Strategy* that allow the reader to gain a better appreciation of "strategy" from a Chinese perspective. Again, chapter titles are in *italics*.

Strategic decision is defined as decision making and planning on problems of war preparation and implementation as a whole. Peng and Yao state that it includes the identification of strategic objectives and strategic tasks, the determination of strategic directions and strategic deployments, and the formulation of strategic plans and strategic preparation of options. It is the

dynamic reflection of the objective strategic situation.[\[132\]](#) Strategic guidelines and actions are broken down into the following components:

- Nature of the action (violent or nonviolent, deterrence or war fighting, positive or negative, decisive or nondecisive, annihilation or attrition)
- Type and style (general or local offensive or defensive, to include strategic direction, area, and services)
- Forms and scope of action (maneuver warfare or mobile warfare, position or guerilla warfare, special operations, regular or irregular operations on interior or exterior lines in land, sea, air, or outer space)
- Patterns and content (blockade or counter blockade, air attack or counter air attack, etc.)
- And process and time of action (beginning of a war, during a war, protracted or quick decision war, withdrawal, pursuit, or decisive battle).[\[133\]](#)

The contents of a strategic plan include strategic judgment, intent, tasks, deployment, support measures, and rear area work. Strategic conductors must employ initiative and a creative spirit according to objective reality.[\[134\]](#)

War preparations are political, economic, military, scientific, and technological preparations made by the state or political groups to restrain or wage a war. There is preparation in peacetime, preparation just before a war, and preparation in the process of war. The development of comprehensive national power becomes the fundamental base for war preparations while scientific and technological preparation becomes the focus of war preparations.[\[135\]](#) The National Defense Mobilization Committee under the State Council and the Central Committee of the CPC are institutions that discuss and coordinate the organizational works of preparing the country for war.[\[136\]](#) The theater of war or strategic war zone is a region for carrying out strategic tasks. It is a level of military command that lies between the supreme command and the strategic operational army group.[\[137\]](#)

War control[\[138\]](#) is an important Chinese concept. Peng and Yao define it as the war conductor's behavior to limit and consciously restrain the occurrence, development, scale, intensity, and outcome of war. The essence of war control is the strategic conductor's initiative in controlling and mastering war. National interests should strictly control military strength. The selection of war means must correspond with the object of interest to be obtained, and the war's conductor should adjust military strategy according to the national interests at stake.[\[139\]](#) Arms control, crisis control, and armed conflict control are all components of war control.[\[140\]](#) 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.[\[141\]](#) 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.[\[142\]](#) 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).[143] The control of armed conflict includes the control of its aim, means, targets, methods, duration, and space of the conflict. [144]

Strategic deterrence control[145] is one method the Chinese may use to win without fighting. They define strategic deterrence control as the 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. Strategic operations and strategic deterrence are dialectically related. The former secures strategic objectives through direct engagement with the enemy on the battlefield while strategic deterrence's objective is to contain the outbreak of war or limit its scope.[146] One must possess a deterrent force, have the determination (the soul of deterrence) to use it, and make approaches urging the opponent to perceive the above-mentioned points, creating psychological pressure on an enemy. [147] One must grasp and understand the basic condition of the deterred opponent and his cultural specifics.[148] The goal is to control the enemy and not be controlled by him. Strategic deterrence requires a combination of nuclear, conventional, space force, information, and People's War deterrence.[149] One must change the opponent's psychological pattern, leave leeway for compromise, and assess the result of deterrence in time. One must also battle factors of uncertainty and the growth or decline of strength, external interference, and psychological imbalance.[150]

Principles of strategic actions are the guidelines to plan and direct the overall situation and the whole process of war.[151] Strategic action guidelines help set a strategic direction, the latter defined as the reflection of the principal contradictions between the PLA and the enemy affecting the overall strategic situation.[152] Strategic conductors are the ones to establish strategic directions. According to the "job description" provided by Peng and Yao, strategic conductors should:

- Have an intimate knowledge of all the circumstances, correctly analyze the international strategic situation, follow developments and changes in the security situation, make detailed analysis of foreign policies and strategic trends, examine military deployments of pertinent countries, correctly evaluate the level of threat to national security and dominant trends, and be knowledgeable of hot issues in disputes and struggles within one's own country[153]
- Keep guidance focused on the main strategic direction; comprehend and deal with operations on the main strategic direction; and utilize creative strategic thinking, careful planning, and clever arrangements to organize strategic coordination and cooperation with other directions to form an overall strategic objective
- Take the subjective initiative based on objective conditions. This includes the other side's war potential and capability, how it could be supported by others, the growth and decline of the two side's military forces, and how a war could be started with the ratio of forces offering one an assurance of victory.[154] War is not only a race of objective or material forces (politics, economy, and science and technology) but also a race of subjective forces such as will, stratagem, initiative, planning, and command[155]
- Be able to control the overall situation and look after all the parts. This requires

knowledge of the impact of time on international strategic situations, the global strategic setup, the strategies of major powers, the level of the threat to national security, the impact of the geographical environment on military actions, and the impact of succeeding stages[156]

- See through the fog of war to predict development trends and seize the most favorable opportunity in time to conduct the offensive resolutely.[157]

Overall objectives, Peng and Yao note, govern the whole process of a strategic situation and directly reflect the political goal of a military operation.[158] It is most likely that China's overall objectives have already been determined. These objectives must conform to China's national interests.[159] It is important to ascertain the success or failure of an objective linked to the center of gravity since the latter can affect the fundamental interest of the overall situation and strategy. In a certain time and space, the manifestation of the center of gravity (COG) includes the acquisition of major strategic goals and action on the principal strategic direction. It is the focal point of confrontation and struggle between China and the enemy. There should be only one strategic COG in a given time and space as there will be no COG if there are too many according to Peng and Yao.[160] COGs are not fixed or unchangeable. Any change in the ratio of forces between the enemy and China may transform the strategic COG. The latter should reflect how to improve China's military capability of winning local wars under high-tech conditions.[161]

Peng and Yao define *Strategic Command* as the organization and guidance of activities performed by the strategic commander and strategic command authorities during strategic operations with the troops under their command. A strategic commander is a command group, not a single person whereas the supreme military commander is a specific strategic commander, not the whole of strategic commanders.[162] Once politicians decide to resort to war, they cannot violate the laws of strategic command. Politicians must not interfere in the normal performance of strategic command activities if the political goal is to be realized.[163]

Strategic command is based on the objective reality of war. This refers to all the objective conditions to include material factors like combat forces, battlefield posture, space-time environment and command system, and spiritual factors such as consciousness, morale, and the feelings of the troops. Subjective factors of strategic command are the directing and waging of war and man's conscious dynamic role in it, a role that can change to some extent the objective conditions.[164]

In planning for war, the strategic commander must seize the strategic pivot. This is the key point having a decisive significance on the overall war situation. The strategic pivot (which sounds similar to the COG concept) can include those stages and processes having decisive influences on the outcome of war. Important battle areas, strategic strong points, and the main strategic direction can all become strategic pivots having a decisive influence on the overall war situation.[165]

Strategic Offensive refers to attacks that help realize the aim of war. The party conducting the offensive has the initiative in selecting the operational direction and the time to commence war.[166] This requires at least relative superiority in certain time and space according to Peng and Yao,[167] who break the strategic offensive direction into four types: point the offensive toward

the center of political domination of the opposing side; point the offensive toward the major economic region of the opposing side; point the offensive toward the major enemy groups; or point the offensive toward the geographically disadvantageous areas of the opposing side.[168] The main strategic offensive direction (one per time period) should try to threaten several strategic targets at once to help maintain flexibility.[169] Main targets should be chosen only after choosing the main strategic offensive direction. Mao believed that the weak enemy should be struck first and the strong enemy second.[170] The major patterns of the strategic offensive are the unidirectional offensive, the multidirectional offensive (composed of the converging, fanning-out, and parallel offensives), the decisive strategic campaign, strategic pursuit, strategic blockade, air offensive, vertical-landing offensive, strategic nuclear assault, and space offensive.[171] The editors noted that

If the strategic offensive aim is annihilation of the strategic groups of the opposing side, such patterns as the multidirectional offensive, the decisive strategic campaign, and the strategic pursuit are usually adopted. When the strategic offensive aim is the destruction of the economic strength and war potential of the opposing side, the patterns of air offensive and multidirectional offensive are usually adopted. When the strategic offensive aim is seizure of the areas under the opposing side's control, the pattern of the naval and air vertical landing offensive will surely be adopted if in areas bordering on the sea or in large islands; and the multidirectional offensive pattern will be adopted if on land.[172]

A successful strategic offensive requires proper preparations and mobilization, a favorable time to go on the offensive (for example, when the enemy is transitioning from the defense to the offense), and sufficient forces to conduct successive attacks and persistent breakthroughs on a defense in depth (which usually requires setting up two strategic echelons and one strategic reserve in the main offensive direction for deployment in depth).[173]

Peng and Yao define *strategic defense* as defensive operations or war stage adopted for war as a whole. Its main tasks are to preserve strategic forces, protect strategic points and important resources, minimize one's losses, wipe out the enemy's troops, and create conditions for moving to the strategic offense.[174]

The major patterns of strategic defense are:

- Defense in place (which includes carrying out the "active offense-defense" or implementing the offensive within the defense)
- Mobile defense (includes the skillful use of timing, terrain, use of stratagems, and planning and organizing the defense among different troops)
- Strategic counterair raids and counterblockades
- Guerrilla warfare (helps establish the initiative and flexibility and includes establishing protracted defensive warfare on interior lines and quick-decision offensive warfare on exterior lines)
- Strategic retreat (a type of strategic maneuver to that starts preparations for a counteroffensive which can be launched quickly or slowly)
- And strategic nuclear counterattack (which does not mean taking a beating passively and requires great timing and coordination with conventional forces).[175]

The strategic defensive system includes combat forces, operational facilities, weapon systems, and all support systems.[176] The essence of the active defense is the offensive defense. Strategic defense doesn't mean waiting passively. Carl von Clausewitz noted that defense is a shield formed of blows delivered with skill, and the enemy's blows must be returned. Antoine-Henri Jomini said passive defensive is doomed, and Friedrich Engels emphasized that active defense carried out by the offensive is the most effective defense. The active defense lays emphasis on the strategic interior-line defense and the exterior-line offense. It is the latter that must be sought.[177]

Strategic Maneuver refers to army operations to move troops and weapons and to shift firepower in an organized way for the realization of certain strategic aims. It is the essential condition for annihilating major enemy groups.[178] Space maneuver will soon include manned, unmanned, and firepower space maneuvers.[179] The main roles of strategic maneuver include: adjusting strategic deployments, changing strategic direction, seizing and creating the opportunity for operations, turning from sitting passively to taking the initiative, and serving as the lever for the shift between offense and defense.[180] Forms of strategic maneuver include ground, air, sea, firepower, and space.[181] Principles of strategic maneuver include seizing the initiative (making full preparations ahead of time; doing the unexpected; and forecasting complicated circumstances); being flexible; strengthening coordination; and combining the pre-positioning of weapons, equipment, and materials with maneuver and combat operations.[182]

Strategic Air Raid (SAR) and Defense against Air Raid (DAAR) are forms of local war under high-tech conditions that may replace ground operations as the main operations to achieve strategic aims. Strategic air raid is a strategic offensive operation that features massive air attacks against an enemy's political, economic and military targets. Strategic defense against air raids are defensive operations designed to resist, counterattack, or protect against an enemy attack.[183] The latter has extended its range to defense in outer space.[184]

Peng and Yao state that penetration under high-tech conditions is possible for those with high-tech weapons, especially those able to control the sea, air, and electromagnetic field (or the ability of the "three controls").[185] To divert the enemy's attention or to deceive him, target demonstration, air route demonstration, altitude demonstration, and radio demonstration would be used. Nearly 70% of the total penetration force should be used against the most important enemy targets in a sudden and fierce attack. Later on one can move to predetermined but intact targets, to newly emerging targets, or to previously attacked targets for complete destruction. A counterattack is a defensive action within an offensive operation.[186]

Defense under high-tech conditions includes striking at command systems, defending against precision strikes, and defending against cyber attacks, reconnaissance, and surveillance. Electronic warfare (EW) will be conducted at the start of a war and throughout it. Strategic weapons include an outer layer fire network to intercept an enemy's high- and medium-altitude air weapons, while ground-to-air missiles and anti-aircraft artillery form an inner layer to counter medium- and low-altitude air raid weapons. Mobile forces made up of ground-to-air missiles and anti-aircraft units will conduct mobile operations as required.[187]

Finally, the editors note that an integrated national strategic air defense system requires a zone defense under the unity of command principle. This should be established

By breaking up the country (theaters of strategy) into several air defense zones based on elaborate planning. With the well-defined three forms of air defense such as the key area air defense (KAAD), field air defense (FAD), and people's air defense (PAD), a complete and yet focused strategic DAAR system should be established through integrating the air defense forces of services and arms as well as units from other military branches.[\[188\]](#)

Strategic Support, the editors note, consists of operational support, logistic support, equipment support, and other such measures.[\[189\]](#) Strategic operational support includes but is not limited to strategic intelligence, communications, electronic countermeasures, meteorology, mapping, jamming, Chinese disruption of enemy C3I systems, and deceiving and bewildering the enemy.[\[190\]](#) Each component has its own unique characteristics which limits the bundling of their capabilities.[\[191\]](#) The universal rule of war to "hit the enemy's vital and weak points" is now applicable to support systems in the reconnaissance, intelligence, early warning, communications, and command and control fields.[\[192\]](#) It was noted that the center of gravity of the overall strategic situation should be strategic logistics support. In terms of space, the emphasis is usually placed on the major battlefield, the main strategic direction and major theaters of operations.[\[193\]](#)

One chapter not listed under strategic guidelines but significant simply for its directions to war conductors is *Conclusion of the War*. The editors wrote that war conductors must be prepared to handle three types of circumstances as the end of a war nears: concluding the war under favorable conditions (the primary goal), in a stalemate, or under unfavorable conditions.[\[194\]](#) With regard to concluding the war the editors again called upon the objective-subjective paradigm:

There are subjective and objective implications for the timing of concluding the war. Objectively, it means that the war has developed to a certain extent and satisfies the conditions for its conclusion within a certain timeframe. Subjectively, it means the choice made by the war conductors on the timing for concluding the war according to changes in war conditions. To end the war, objective conditions and proper timing are equally important.[\[195\]](#)

That is, one must create conditions for ending the war when in unfavorable circumstances using subjective creativity. One must seek partial military victories.[\[196\]](#) If national interests are maintained, the editors note, then a war is concluded under favorable conditions even if some aims aren't achieved.[\[197\]](#)

Taiwan

No formal section on Taiwan was included in *The Science of Military Strategy*. However, as one of the key topics always on China's radar screen, the issue came up continuously in the book and a summarized treatment is offered here.

Peng and Yao state that Taiwan was founded due to a regime change on a piece of China's sovereign land. This fact does not allow for a claim of sovereignty over this territory by anyone other than China nor for any claim for status as a subject of international law. Taiwan's status is as

an inalienable part of China. It is essentially an issue of China's internal affairs. Taiwan, Peng and Yao note, is important since it is a key area for sea routes in the Pacific, is a sea transport hub connecting Shanghai and Hong Kong, is where China can breach the chain of islands surrounding it in the West Pacific, provides a maritime defense system in depth, is a large area of water territory with rich reserves, and guards its trade routes from exposure and surveillance.[198]

China aims to resist aggression, maintain unity, oppose separation, and safeguard the motherland. If there is any foreign occupation of Taiwan, or if the Taiwanese authorities refuse to conduct negotiations with the mainland to settle the reunification issue, then the Chinese government would have to resort to forceful measures, including military force. China abides by the "one China" principle, and wants to solve the Taiwan issue through "peaceful reunification, one country, two systems." [199]

Earlier in The Science of Military Strategy, Peng and Yao had addressed the sovereignty issue. They noted that if hostile forces such as religious extremists, national separatists, and international terrorists challenge a nation's sovereignty it could be considered as firing the first shot on the plane of politics and strategy.[200] Strategic conductors will have the chance to fire the first shot on the plane of tactics if territory or sovereignty is disrupted, they note. Local war always has the potential to become unlimited depending against whom the attacks are initiated. [201] Thus Peng and Yao make it clear just how special Taiwan is to the PLA and what strategic implications the island holds.

Conclusions

Peng and Yao's book has no formal chapter devoted to conclusions. However the book did have a Postscript. It stresses what the editors deemed important as they concluded their lengthy work. A set of general conclusions that can be drawn from a review of the book's contents follows the postscript discussion. Finally a comparison is made of the major elements of this book as compared and contrasted against the US theory of strategy. Other important points in The Science of Military Strategy can be found in the concluding chapter of Decoding the Virtual Dragon.

Postscript

Peng and Yao stressed three issues in the postscript. They are the essence of war, the laws of war, and the requirement of the science of military strategy to improve the theoretical system of strategy. The latter issue focused on providing new thoughts for winning local wars under modern conditions. In the editors' opinion, war and strategy have "never experienced such dramatic and profound changes before." The direction of these developments is difficult to predict and their nature is difficult to recognize according to Peng and Yao. This implies that the book's results can only be tested or improved by practice. Further, the postscript states "dramatic developments in the practice of wars urgently require new theoretical explanations about the emerging situation." In the opinion of the editors, the RMA and high-tech local war have produced new problems and new conclusions for evaluating the laws of war and the conduct of war.[202]

Review of the Book's Contents

The editors appeared to have taken several favorable steps toward improving the theoretical system of strategy in their work. Noting that military science is characterized by antagonism,

politics, comprehensiveness, stratagem, practice, and prediction, they highlighted the need for each to work in harmony throughout the book. The editors focused on the characteristics of strategic thinking—totality, confrontation, certainty, foresight, creativity, and inheritance—and this sharpened the reader’s thoughts on harmony of effort. The editors’ development of a host of applied strategic issues (strategic decision, strategic command, strategic maneuver, strategic offense and defense, strategic air raid and anti-air raid, strategic deterrence, strategic action principles, and strategic support along with war preparation, war control, and war conclusions) indicated their continued comprehensive approach to the issue of adopting strategy to high-tech war.

The editors identification of two issues, change and new problems, may be the reason behind this new discussion of strategy. It is also interesting that the PLA has added a few new types of “comprehensiveness” into their planning. No longer does CNP seem to be enough. The one that stands out of course is comprehensive cyberized war although the editors did little more than just mention the concept. To old China hands, the other items on the “comprehensive list” developed for this chapter (comprehensive strategic targets, comprehensive national defense construction, comprehensive confrontation capacity, etc.) may be old news. They do remain indicative of the truly holistic strategic approach that PLA theorists take into account when considering their environment.

The editors integrated several issues into their narrative that ring familiar to Westerners. These included concepts such as centers of gravity, asymmetric thinking, national interests, and principles of strategic action. Other issues were more Chinese and Marxist in nature and less easily understood, such as objective versus subjective thought; the nature, form, means, application and time features of strategy; and the division of strategy into basic and applied aspects. The Western reader is left with a feeling that the Chinese concept of strategy is much more comprehensive than Western strategic concepts. Western readers should also be impressed by the careful preparation and research of this work that allowed for their entire editorial staff to explain issues clearly.

Readers are also left with the impression that, speaking in very general terms, there are three levels of military art, strategic, operational, and tactical, and each level has a country of expertise. Countries can learn from one another in this regard. For strategic issues, the Chinese have a long historical perspective and expertise. *The Science of Military Strategy* only adds to their legacy in this area. For issues of operational art, the Russian military developed some of the more creative ideas such as the operational maneuver group, and they continue to focus much of their writings on this level of war. And for issues of tactics, the US armed forces, based on a long practical history in this area, remains the resident center of expertise and knowledge.

Summary Comparison of Chinese and US Strategic Views

The definitions of the military term “strategy” in China and the US have some similarities. There are several distinct differences, however, in the logic and structure used to apply the term. It should be emphasized, however, that two distinct and different institutions were accessed to analyze the meaning of strategy. One is a branch of service (the US Army War College, an army institution) and one is a representative of an armed forces as a whole (China’s Academy of Military Science).

The differences demonstrate various approaches in analysis, understanding, development, and application of the term strategy in China and the US. These differences are:

- Basis for analysis: the Chinese apply subjective criteria to objective conditions in the development of strategic judgments. This is most evident in the widespread use of stratagems, a creative form of subjectivity. The US views strategy as the relationship among ends, ways, and means. Stratagems are seldom mentioned in the US understanding of strategy.
- Comprehensive focus: China takes a comprehensive view of most issues, offering holistic assessments of national power, cyberized war, and many other issues as listed in this document. US views are more focused and less holistic although the term comprehensive is mentioned. Henry Eccles, for example, described strategy as the comprehensive direction of power to control situations and areas in order to obtain objectives.^[203] There is seldom, however, a further reference to what “comprehensive” means.
- Strategy and military science: China tends to take a more scientific view of strategy. There is a “science of strategy” that divides strategy into basic and applied categories. There is no such subdivision of the term in US parlance.
- Role of specialists: In the US, the viewpoints of several famous strategists serve as the basis for the understanding of strategy. The works of foreign strategists in this regard (Clausewitz, Jomini, Liddell Hart, etc.) are probably discussed more than the works of US strategists. In China, foreign strategists do play a role. However, the two most important military writers with an influence on strategy appear to be Sun Tzu and Friedrich Engels, the latter for his work on People’s War theory and the active defense concept. Mao was the integrator of their thoughts and remains on a par with both men concerning strategic thought in Chinese eyes.
- Strategy versus operational art and tactics: A point of interest is that China, for the past 30 years, has not been involved in the continental deployments of forces as has the US nor been engaged in combat with the same frequency. As a result, the US is much more focused (and most likely much more adept) at operational art and tactics. China, less battle-proven, perhaps focuses more on strategy because it has not been engaged in conflict. Political, economic, and now information strategies occupy much of the military academies time and effort.
- Hard versus soft strategy: Chinese strategy, due to its subjective focus, places emphasis on both the use of hard power and the use of soft “stratagem theory.” That is, the Chinese explore how stratagems, culture, and law can be used as adjuncts to hard power. US strategy addresses soft power adroitly but still places more emphasis on hard power. In fact the term power is used in the JP 1-02 version of strategy’s definition. This reference to power is also apparent in the most often used US definition of strategy, that being “the relationship among ends, ways, and means.”

The US Army War College, of course, does possess other methods for examining strategy and remains a preeminent US installation dedicated to understanding strategy’s many aspects. The purpose of this chapter was to emphasize differences in the Chinese and US approaches and not to

negate in any way the major contributions made by the War College to this subject. For example, one such method to analyze strategy at the War College was by categories and another method was via premises. Categories were listed by J. Boone Bartholomees in the US Army War College Guide to National Security Policy and Strategy. He categorized strategy's aspects as follows: declaratory, actual or ideal; sequential, simultaneous, and cumulative; organizational and hierarchical; and miscellaneous, alternative, and possibly-strategic concepts.[\[204\]](#) US analyst Harry Yarger, writing in the same volume, listed "premises" of strategy. They are: being proactive and anticipatory; knowing what is to be accomplished (the end state); identifying an appropriate balance among objectives sought, methods to pursue the objectives, and resources available; allowing political purpose to dominate strategy; noting that strategy is hierarchical and comprehensive; developing strategy through analysis and knowledge of the situation; and understanding that some risk is inherent to all strategy.[\[205\]](#)

Author David Jablonsky of the US Army War College stated that people know from experience that there are limits to the scientific approach when dealing with human endeavors and "as a consequence, they can appreciate the art of mixing ends, ways, and means, using for each element the part subjective, part objective criteria of suitability, feasibility, and applicability—the essence of strategic calculation."[\[206\]](#) Thus he comes closest to the Chinese definition of strategy. He adds:

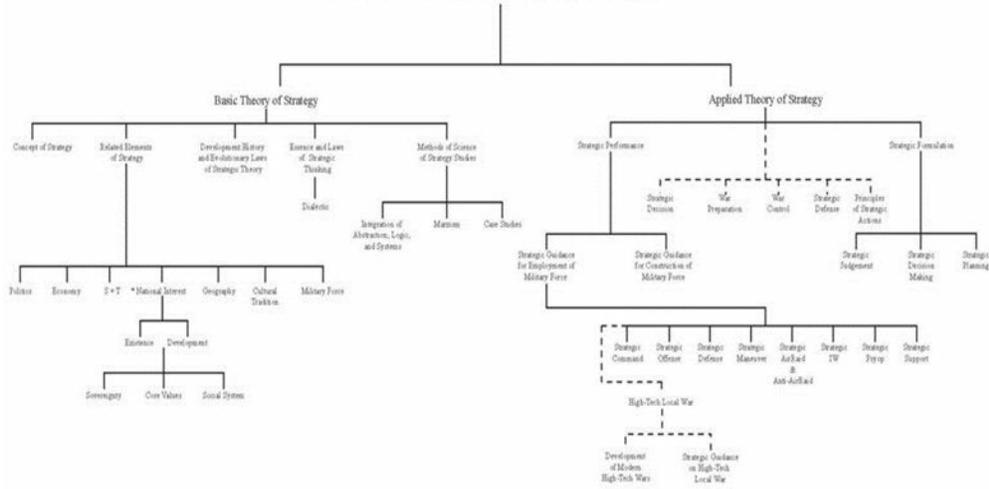
Thus, the mix of ends, ways, and means at the national military strategic level will affect directly (and be affected by) the same paradigm operating at each level of the vertical continuum. Adding to the complexity is the interplay on the horizontal plane of national military strategy with the other strategies derived from the elements of national power, each operating within its own strategic paradigm and all contributing to the grand design of national strategy, as that strategy evolves within its own overall mix of ends, ways, and means.[\[207\]](#)

How US political, economic, and military strategies interact on horizontal and vertical planes is one issue. How US national military strategy interacts with the Chinese outline of military and national strategy presented above is quite another, one that will require much analysis, foresight, and simulation on the part of US strategists.

Diagram 1A

Science of Strategy

“Military science studies the laws of war, laws of the conduct of war,
and laws of the evolution of strategic thought”



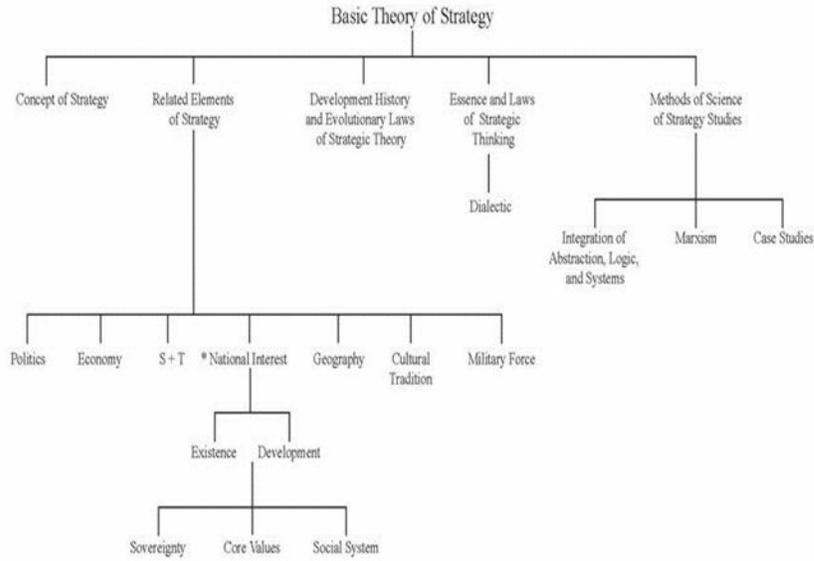
* National Interest is both the starting point and destination of Military Strategy

Part One - Basis of Science of Strategy
 Part Two - General Laws of War & Conduct of War
 Part Three - High-Tech Local War & Guidance on it

Diagram 1B

Science of Strategy

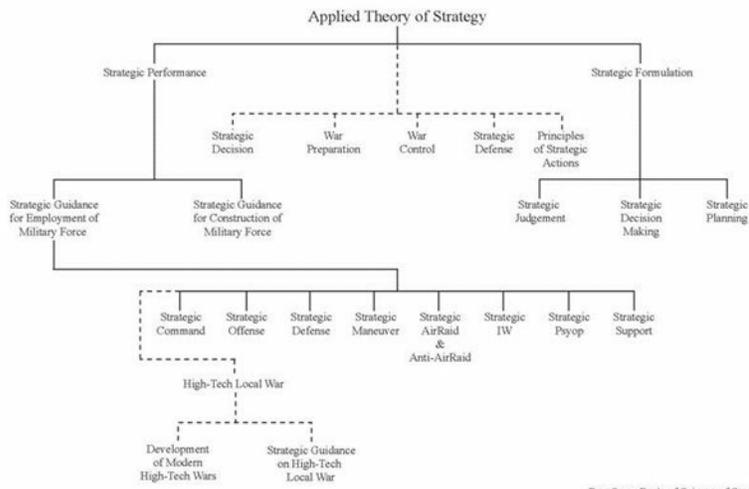
“Military science studies the laws of war, laws of the conduct of war,
and laws of the evolution of strategic thought”



*National Interest is both the starting point and destination of Military Strategy

Diagram 1C

Science of Strategy
 "Military science studies the laws of war, laws of the conduct of war,
 and laws of the evolution of strategic thought"



Part One - Basis of Science of Strategy
 Part Two - General Laws of War & Conduct of War
 Part Three - High-Tech Local War & Guidance on it

CHAPTER TWO: THE SCIENCE OF INFORMATION OPERATIONS

This chapter summarizes Xu Xiaoyan's article "Advancing the Science of Information Operations," which was published in China Military Science, Volume 3, 2004.[208]

Introduction

In July 2006, China's Xinhua Domestic News Service, recounting the achievements of the People's Liberation Army (PLA) in the past five years, noted that progress was made in the "principal contradictions, development concept, and relevant countermeasures in the informatization of our armed forces, the relationship between development by leaps and bounds and sustainable development, and the development of the informatization battle capability in our military units." [209] In theoretical work, important developments were made in the new or cross disciplines of international military science, military sociology, and, most important for this chapter, the science of information operations (SIO). [210]

Major General Xu Xiaoyan, former head of the Communications Department of the Chinese General Staff, is an experienced author on the topic of SIO. In 2002 he wrote a book titled The Science of Information Operations. In 2004 he published an article on SIO in the journal China Military Science. This chapter will review Xu's journal article as it demonstrates the extension of the military science paradigm (basic and applied theory) in the previous chapter. Since SIO is a concept that the US military does not employ, it provides new content for US consideration.

Xu defined what he meant by the science of information operations and outlined many details of such an academic system. He believes that the science of IO is now mature and that an academic system for its study must be established. Xu stated that it is imperative for the PLA to make preparations now for combat under new (IO) conditions. His SIO article demonstrates the extent of that urgency. The Chinese hope that this new science will meet the innovative needs of the PLA and enable it to organize and win at informationized warfare.

The Science of Information Operations

The science of IO is a relatively new branch of Chinese military science. It is defined as

A branch of military science that studies the rules of IO and gives guidance to the practice of IO. Its main tasks are to use scientific methods to reveal the essence of IO and the influence of various objective factors on IO, the operational mechanisms and internal rules for command and control of IO, and practical activities thus providing theoretical guidance for the practice of IO." [211]

Xu states that three conditions are required to create an academic discipline such as SIO. They are a common understanding of the unique qualities of an area, a more unified understanding of the structure of the discipline within the area, and the dissemination of statements compelling those in academic circles to acknowledge the existence of the discipline. These three conditions

are now present in the Chinese system, and the time appears ripe to conduct the study of SIO. The construction of a system for an information-based, military-academic discipline within military studies also promotes topics that encourage military reform.[\[212\]](#)

The science of IO addresses a way to develop methods to win future informationized wars. Chinese theorists describe the theoretical system of the science of information operations (IO) as composed of three parts: basic IO theory, applied IO theory, and technical IO theory. (See Diagram 2 at the end of this chapter.) Basic IO theory reveals the laws that govern IO, studies the rules and principles of IO, and provides structure for the organization and command and control of IO. Applied IO theory reveals the special features of organizing and implementing various types of IO and studies rules and operations of IO. It is the concrete implementation of the basic theory. IO technical theory reveals the overall mechanism and development of IO technology; studies the principles and methods of implementing, building, and developing IO technology; and plays a role in providing technological support for basic and applied theory.[\[213\]](#) The science of IO is different from the science of military strategy since strategy does not have a technical component.

Major General Xu stated that a second level of disciplines also needs to be developed for IO. He described what he termed “branch disciplines” that should be created. They are command and control during IO, IO technology, IO transmission, IO intelligence, IO countermeasures, IO buildup, IO strategy, and IO training.[\[214\]](#)

IO’s theoretical research aims to explore and discover the various phenomena and patterns of IO.[\[215\]](#) IO not only sits at the center of all activities of two warring sides on today’s battlefield but, due to its nature, is more independent and unique than any other academic branch in Xu’s opinion.[\[216\]](#) IO’s logical start point is information countermeasures or confrontation measures which are activities designed to oppose hostile forces IO activities[\[217\]](#)

Basic IO Theory

There are twelve sub-elements of basic IO theory. They are concepts, weapons and armaments, strength, categories, principles, command and control, combat methods, organization and planning, resource management, logistics support, education and training, and result appraisal.

“IO Concepts” was also a sub element of the science of military strategy and includes definitions for the terms IO, information warfare, and informationized war. “Concepts” reveals the basic characteristics of IO and the status and role of IO in war.

“IO weaponry” is “the general name for various weapon systems and armaments that are built with information technology as the core and are directly used to destroy, damage, and weaken information and information systems on the enemy side and to protect the information and information systems on one’s own side.” Combat forms (weapons) that Xu lists are those that the US associates with the capabilities of IO (some were in past US IO definitions: some are in current definitions): intelligence warfare, computer network warfare, electronic warfare, psychological warfare, and physical destruction warfare. IO weaponry also addresses types of destructive effects, types of platforms, and degrees of versatility of IO weapons.[\[218\]](#)

“IO strength” refers to all available forces for IO, both actual and potential. Stating that there

are IO forces in the army, navy, air force, and second artillery corps, Xu defined the characteristics (information reconnaissance, attack, and defense), scale (strategic, campaign, and tactical IO forces), mission (command, attack, defend, and support forces), and force formations (military services and branches, armed groups, or IO missions).[\[219\]](#)

“IO categories” refers to actions defined by certain standards. These actions include intelligence, electronic, psychological, computer network, and physical destruction warfare methods. The latter focuses attention on the destruction of information facilities. Definitions are listed for each. They are:

- Intelligence warfare: the ability to seize information supremacy
- Electronic warfare: the electromagnetic fight for use of electronic equipment and devices
- Psychological warfare: a type of warfare that adopts special methods and means to affect, constrain, and change the thinking, feeling, and behavior of the enemy through psychological factors and at the same time consolidate the psychological defense of one’s own side
- Computer network warfare: IO between two warring sides to seize domination of computer operations through weakening and sabotaging the enemy’s computer network systems
- Information facility destruction, also called physical destruction or hard destruction warfare: use of IO weaponry as well as military troops and firepower for destruction and damage purposes while protecting one’s own side.[\[220\]](#)

“IO principles” are the basic norms to follow in the conduct of IO. They are concrete forms of the laws of IO that include peacetime and wartime integration of actions to ensure preparedness for emergencies, unified command and coordination, military and civilian integration for full-dimensional force deployment, simultaneous offensive and defensive operations that include hard and soft means, strict security, flexible use of combat methods, and integrated support and well-planned actions.[\[221\]](#)

“IO command and control” refers to the organization, command, and control of IO. Commanders compose the main body of this group, and troops and weapons are the subjects of their commands. They perform missions. The command automation system is the means to perform command and control, and the basic element of command and control is information flow. The scope of command and control is the informationized battlefield.[\[222\]](#)

“IO command methods” are the methods to conduct IO. They include methods at the strategic, campaign, and tactical levels and include characteristic actions such as information reconnaissance, offense, and defense. IO can also be used in landing operations, cities and mountains, air attacks, special operations, counterair raids, border counterattacks, and antilanding operations.[\[223\]](#)

“IO organization and planning” is the scientific planning and arrangement for IO-related military actions. It is the core of command and control. It includes collecting and processing intelligence, IO decision making, IO planning, and IO combat completion. It also refers to the

actions of commanders and command organs that collect or expose intelligence after receiving missions. Based on this data, information is processed, sorted, and analyzed further to provide decision makers with the required data to ascertain objectives and activities. Strategic IO decisions are thus turned into combat actions.[\[224\]](#)

“IO resource management” is the management of the battlefield spectrum as well as data and civilian information resources. The term spectrum refers to the management of advanced technical means and to flexible tactical measures for managing and using the electromagnetic spectrum to achieve information supremacy. Data refers to the transfer, processing, and use of IO data to form an “information capacity” for winning operational victories. Civilian IO resources must manage civilian information that is related to IO mobilization and logistical activities.[\[225\]](#)

“IO logistics support” refers to providing information resources, material, equipment, and technical support to IO combat activities. Support can be independent in form for each branch of service or unified for all services. Methods include regional, delivery, distribution, network, and long-distance mobilization support.[\[226\]](#)

“IO education and training” refers to activities associated with IO knowledge and theory. Training must be focused on confrontation and the enhancement of joint actions. Rules and regulations must be perfected based on top-down design. Methods of IO education and training include theoretical discussions, simulations, online confrontations, training at military bases, and war games with troops.[\[227\]](#)

Finally, “IO results” must be evaluated. To do so Xu recommended the examination of several issues. They are: evaluating IO characteristics via four categories (reconnaissance, offense, defense, and support for IO); evaluating IO forms via the five forms (intelligence warfare, electronic warfare, etc.); evaluating IO confrontation targets via information evaluation, information systems effectiveness, and information weaponry appraisal; and evaluating IO methods via practice assessment, mathematical analysis, and computer simulation. Implementation of these results relies on decisions regarding the method of appraisal, the organization of the implementation of appraisals, and the analysis and use of conclusions reached.[\[228\]](#)

Applied IO Theory

Applied IO refers to IO conducted by the specific military services:

- Army IO is a series of combat actions carried out by the army’s IO force, on land or on islands. It focuses on the army’s campaign and tactical intentions and is accomplished either independently or in conjunction with other services. Army IO includes armor, artillery, air corps, signal, antiaircraft, electronic confrontation, engineering, and chemical defense corps IO.
- Navy IO is a series of combat actions that serve the navy’s campaign and tactical intentions. It includes submarine, surface fleet, naval air force, coast guard, and marine IO theory.
- Air force IO is a series of combat actions in the course of air battles to serve campaign or tactical intentions. IO theory includes the aviation and air defense corps as well as radar units.

- Second artillery corps IO is a series of combat actions taken in the course of performing a nuclear counterattack operation or a conventional missile operation to serve general military intentions. IO theory includes short, medium, long-range, and intercontinental missile corps.[229]

Xu listed only joint theory as a sub-branch for applied IO theory in contrast to basic theory's many sub-branches. Joint IO theory included theories for island blockades, firepower and island attacks, resisting air raids, border counterattack campaigns, and resisting enemy landings.[230] Individually, each theory is comprised of the following IO aspects:

- Blockading islands: studies IO use to form a blockade, to seize control over blockaded areas, to maintain a sustained three-dimensional blockade, and to add support to resisting enemy antiblockade operations
- Firepower attacks: studies IO use to fix attack targets, conduct firepower attacks, resist enemy firepower counterattacks, and assess results
- Launching attacks on islands: studies IO use in early aspects of a campaign, during force assembly and maritime navigation, and during landing and on-island operations
- Resisting air raids: studies IO use during air defense operations, during actions to resist enemy air attacks, and during counterattack operations
- Border counterattack campaigns: studies IO use during combat force campaign mobilization, preemptive actions, defensive battles, counteroffensive operations, and campaign results
- Resisting enemy landing: studies IO use in preemptive resistance actions against an enemy, during battles when attacking enemy forces in assembly areas and when loading, during navigation, during battles to defend islands and key coastal positions, and in support of antiair drop and antiraid actions.[231]

Technical IO Theory

A third aspect of the science of IO is the technical aspect. Si Laiyi edited a 1998 book on this topic titled The Science of Information Operations Technology. Thus the topic is now at least nearly ten years old.

Xu subdivided technical IO theory into basic, main, and comprehensive applied technology. Basic IO technology is the technology for the production of components for IO weapons and devices. Main IO technology is the development, design, and production of equipment and systems that collect, transfer, process, reproduce, and control information (thus the term "main"). Comprehensive applied IO technology is that which integrates and applies IO technical systems. Comprehensive technology further integrates elements of basic and main IO technology.[232]

Of the three components of IO theory, Xu only further subdivided main technical IO theory. The areas are as follows:

- Information collection technology—expands the function of human sensing organs and enhances the human capability of perceiving and understanding things

- Information transmission technology
- Information processing technology—the integration, categorization, calculation, storage, etc. of information to support planning and decision making processes through simulations, comparisons, and so on
- Control technology—control via the input of commands
- Electronic countermeasure technology
- Network confrontation technology—intercepting, utilizing, corrupting, and damaging the enemy’s information and using false information, viruses, and other means to sabotage normal information system functions through computer networks
- System integration technology—coordination and optimization one strives to achieve the general objective of IO.[\[233\]](#)

Xu further stated that an IO technical development strategy was required. This strategy would plan and guide the general development of IO technology. Further,

The science of IO will integrate the key development points of the national information industry and the development trends of information warfare currently in our armed forces and in foreign armed forces and put forward the key points, policies, methods, and main measures that should be adopted for developing IO technology, including computer and artificial intelligence technology, battlefield information sensing and collection technology, communications and networking technology, and information confrontation technology, in accordance with the strategic requirements of our armed forces’ informationization building and the requirements for winning informationized warfare.[\[234\]](#)

Xu’s Recommendations/Conclusions

There were several recommendations that Xu made in the article. First, he noted that breakthroughs must be made as quickly as possible in the science of IO. The PLA cannot just copy what other armed forces are doing. The PLA has its own strategic guidance, objectives, and developmental foundation, and it must apply these issues in an asymmetric manner. The PLA needs to develop theories about space IO and computer network warfare that create breakthroughs in these theories as well.[\[235\]](#)

Second, Xu noted that the PLA must quickly build platforms with integrated hardware and software for the science of IO. Only with high quality academic platforms can new scientific theories of IO be developed. Training and experimental bases are needed to include an all-army research center to advance informationization and IO in the PLA.[\[236\]](#)

Third, Xu noted that creative guidelines must be developed that include establishing a systematic science of IO. The system must follow strategic thinking regarding the revolution in military affairs (RMA), act on military strategic principles from the Central Military Commission, and adhere to general ideas of scientific proof, long-term planning, and incremental implementation. Military communication theory, command automation theory, electronic confrontation theory, and military intelligence theory are the basic developmental requirements to properly address the science of IO.[\[237\]](#)

In addition to providing three recommendations, Xu also developed three problems for the PLA to solve. They are:

- The necessity to stop neglecting applied theory and only attaching importance to basic theory
- The necessity to stop neglecting practical verification while only attaching importance to theoretical research
- And the necessity to stop neglecting the settlement of major difficult issues (in preparing for military struggle) while only attaching importance to researching general issues. Concepts must be changed into actions.[\[238\]](#)

Xu concluded his article by noting that the basic principles of the science of IO must include integrating theories (via systems theory) into the IO field, practicing IO in accordance with the needs of the armed forces, and developing science to meet the needs of the armed forces. The science of IO must objectively “reflect the character of IO and the rules that govern the development of such military operations...we should strive for unity between its character of development and its character of being realistic.”[\[239\]](#)

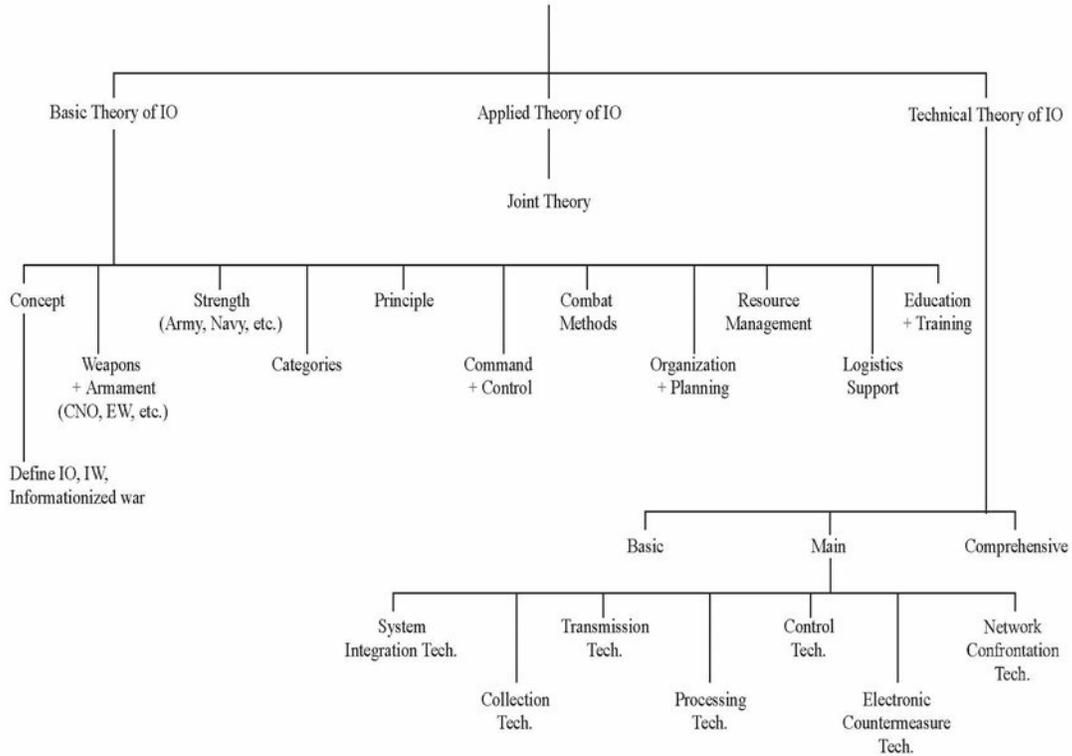
The issue of theory and practice is an important one. The PLA has not fought as extensively as have many Western governments and thus has only limited experience in operational art and tactics. But they have developed lots of theory during these years. If Xu’s suggestions were accepted (he wrote the article in 2004), then one might expect to see more active reconnaissance and intelligence activities on the part of the PLA (as seems to be occurring!) than on the pure development of theory.

There were other areas of interest in Xu’s discussion of the science of IO to point out. First, the focus of the means of physical destruction on “information facilities” is of interest. It is not known if these are military or civilian facilities but the intent to go after IO targets and destroy them is of interest. Second, there is a huge difference in the subdivisions of basic and applied theory if one compares the Chinese version of the science of military strategy with the science of IO. The former has several subdivisions under “applied theory” which indicates that military strategy has an active role to play in peacetime. Applied theory means theory that is being practiced. With the science of IO, the emphasis is reversed. There is much more emphasis on basic theory than on applied theory. This indicates that the PLA either is still considering how to implement the science of IO or it is a classified section. In any regard, Xu’s recommendation to increase the PLA’s emphasis on applied theory should not be forgotten. Third, much of the focus of the PLA’s joint theory applied aspect (the sole subdivision of applied theory) was on islands. This is not usually the case with Western nations and reflects not only China’s Taiwan problem but also probable future worries over sea lane chokepoints.

Studying the Chinese method of military science and its subdivisions by category is an excellent way for US theorists to take a more comprehensive look at various fields of study. Our historical experience and methodologies do not lead us down the path of basic and applied theories. The latter are beneficial in causing theorists to develop a more comprehensive and methodological look at a topic and its various subtopics and to develop more precise terminology.

Science of Information Operations (IO)

“Branch of military science that studies the rules of IO and gives guidance to the practice of IO”



CHAPTER THREE: CHINA'S REVOLUTION IN MILITARY AFFAIRS AND INFORMATION OPERATIONS

This chapter summarizes key points from editor Shen Weiguang's book On the Chinese Revolution in Military Affairs, 2004.[240]

Introduction

A topic that has received much attention during the past ten years is the revolution in military affairs (RMA). The US took the initial lead in developing this concept and its related technological effort. For example, two of the US armed forces most prominent military journals, Joint Forces Quarterly and Parameters, have published more than fifty articles on the concept of the RMA in the past decade.

Fewer people in the US, however, have tried to define the concept and make sense of it. A check of the US Military's Dictionary of Terms and Concepts reveals that, as of December 2006, the term still has not been officially defined. Steven Metz and James Kievit defined RMA in 1995 as a "discontinuous increase in military capability and effectiveness" arising from simultaneous and mutually supportive changes in technology, systems, operational methods, and military organizations.[241] Jeffrey Cooper, also writing in 1995, added that changes in the tools of war, changes in the behavior of militaries, and changes in the nature of warfare are the keys to understanding a RMA.[242] Andrew Krepinevich wrote in 1994 that the RMA was what occurs "when the application of new technologies into a significant number of military systems combines with innovative operational concepts and organizational adaptation in a way that fundamentally alters the character and conduct of conflict." [243] Finally, in 1999 Richard O. Hundley of RAND defined RMA as "a paradigm shift in the nature and conduct of military operations which either renders obsolete or irrelevant one or more core competencies of a dominant player; or creates one or more new core competencies, in some new dimension of warfare; or both." [244] Others have added slightly different twists to the concept.

The Chinese military has studied the meaning and impact of the RMA for the past decade as well. Like the US, the Chinese have been reluctant to offer an official definition, relying in the 1990s on the definitions of Western specialists such as Krepinevich and Hundley. While it might be assumed that China's understanding of RMA would thus be similar to that of the US or other nations, it is not. For example, in 2001 retired Chinese Major General Wang Baocun defined the term as a process of military informationalization where theory and practice are the focus. He added that Chinese progress toward an RMA is signaled by its C4I modernization, network-based war-gaming, information warfare (IW) personnel training and field exercises, and informationalized equipment.[245] Thus Wang's Chinese perspective indicates that the information revolution is the key component of the current RMA.

For purposes of this chapter, the RMA focus is on a 2004 Chinese book titled On the

Chinese Revolution in Military Affairs. A number of influential Chinese strategic, information warfare, and media specialists (which includes the authors of the much publicized Unrestricted War) provide important RMA insights to the volume. The book provides one of the most comprehensive Chinese RMA conceptualizations to date and provides an updated assessment of the RMA's impact on strategy, control, and innovation. The traditional US focus has been on technology and capabilities. Common ground with the US is found over organizational changes and information technology.

The US and Chinese differences over RMA benefits are intriguing. The differences in emphasis most likely are a direct reflection not only of capabilities but also of culture. The US lead is in technology while the Chinese rely on theory and strategy to enable (in their opinion) their inferior force to overcome US superiority. One Chinese author in the book under review noted that the RMA is really a cognition system revolution and a new phase in military strategy research. Another author in the volume noted that the essence of the RMA is the reflection of informationization (the Chinese preferred term for cyberization or digitalization) in the military field. Yet another of the work's authors added that the RMA involves a series of changes to military theory, methods of operations, weaponry, systems organization, command organization, and so on, an understanding closer to most US RMA concepts.

This chapter's findings on China's RMA focus may surprise some US analysts, as the Chinese try to develop an RMA concept with Chinese characteristics. As one Chinese general wrote about the information warfare aspect of the RMA:

Only with superior thought processes and superior moves, and by seeking a developmental strategy of "imbalance" will we truly be able to avoid traveling the "path that the enemy expects." In the realm of information warfare (IW), trying to keep up with the Jones' by developing whatever they possess will lead to falling into traps set by others; regardless of how rapidly we develop, it will still be hard to escape being controlled by other people. [246]

This chapter will explain what new paths the PLA is seeking. Their emphasis on superior thought processes, their development of information age strategies, and their focus on concepts such as control, perception, and cognition that have led to new theories for offensive and defensive activities. The resulting "new" fog of war they intend to cast may be something never before contemplated.

Early Chinese RMA Thoughts

The Chinese apparently utilized the term "military revolution" interchangeably with the term RMA in the mid-1990s. A 1996 Chinese article on IW theory, for example, defined a military revolution as "a reflection of social, economic, and scientific and technological changes in the military field." [247] Another 1996 article defined a military revolution as "a major qualitative change which can correctly integrate, with good timing, advanced technologies and weapon systems with new military theories and military establishments; bring permanent changes to modes of operations; considerably improve military efficiency; and enhance the combat effectiveness of armies by several orders of magnitude." [248]

One RMA definition reportedly in the 1997 Chinese Military Affairs Dictionary, defined

RMA in the following way:

Starting from the premise that social transformation is a prerequisite for a revolution in military affairs, the military field experienced a series of fundamental and profoundly influential transformations. It is primarily a reflection of qualitative changes in military technology, weapons and equipment, unit structure, war fighting methods, and military thought and theory.[\[249\]](#)

A year later, the tone and substance of Chinese articles on the RMA became more cautious. One article noted that “a mammoth revolution currently underway in the military sphere is producing an unprecedented impact on, and shock waves in, man's military activities.”[\[250\]](#)

Several Chinese authors in On the Chinese Revolution in Military Affairs note that China must find its own unique techniques and skills during its investigation of the RMA.[\[251\]](#) The country should not simply follow Western thinking and add only Western developments and technologies to the existing framework since

Due to their different economic and scientific development levels, as well as their different cultures, traditions, and ways of thinking, different countries will be subjected to different impacts produced by military revolutions; as a result, they will adopt different approaches toward new things and accept the new military revolution in varying degrees. Therefore, there will be a growing trend toward diversification in the pattern of war at the initial stage of the military revolution.[\[252\]](#)

China’s RMA Theory in 2004: Now with Chinese Characteristics

A number of RMA-related articles were written for Chinese military journals from 1999 to 2004. However, in 2004 Chinese publications focused so intensely on the RMA issue that the topic appeared to be a directed PLA leadership discussion forum.

On the Chinese Revolution in Military Affairs was selected for review in this chapter because it has a sharp strategic and information focus. Chinese subject matter experts authored several of the chapters, further increasing the book’s valuable insights. As Chinese authors Major General Niu Li, Colonel Li Jiangzou, and Major Xu Dehui (all of the Communications and Command Institute) noted in 2000:

Traditionally, Oriental people emphasize stratagems, and Occidental people emphasize technology...Occidental soldiers would seek technological means when encountering a difficulty, while Oriental soldiers would seek to use stratagems to make up for technological deficiencies without changing the technological conditions.[\[253\]](#)

Thus this book may provide hints as to the strategies used when applying IW/IO.

On the Chinese Revolution in Military Affairs has several intriguing sections of value for US policy planners and military theorists that illuminate how Chinese thinkers combine strategy with

electronic data. An example is a statement by Major General Li Bingyan, a stratagem specialist, regarding the flood of information available to modern analysts:

In the information age there is information excess, information overload, information surplus, information inflation, and information overflow, and that is a new factor of war friction. One philosopher said that absolute light and absolute darkness have the same effect—we cannot see anything. With information overflow, the modern battlefield is more richly colorful and an area for cunning and deception.[\[254\]](#)

Other authors presented equally stimulating thoughts. Two such ideas were on the new objective of war and China's strategic frontiers, respectively:

War with the objective of expanding territory has already basically withdrawn from the stage 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. Although this kind of war really does not require that military actions be synchronized with the flow of global financial capital, yet it will influence and control this flow, and it does require that military actions take place within a few days or even a few hours.[\[255\]](#)

Our strategic frontiers must be greater than our territorial frontiers; they simply cannot be smaller than our territorial frontiers. For a country without ambition and with unclear security and strategic objectives, the RMA is a march with no objective.[\[256\]](#)

In addition to such key assessments, this RMA book also includes a host of definitions of military concepts, several Chinese viewpoints on the war in Iraq, and the RMA's impact on decision making.

Thirteen different Chinese authors wrote chapters for this book. Some of the chapters were actually articles that the authors had published a year or two earlier in Chinese journals. The chapter titles and authors are listed here not only for ease of reference but also to familiarize readers with this list of professional PLA RMA specialists.

1) "Applying Military Strategy in the Age of the New Revolution in Military Affairs" by Li Bingyan. He is the senior editor of the Chinese People's Liberation Army's (PLA) newspaper Liberation Army Daily. Li is a Major General and an expert in military strategy. The author of several prominent military books, Li's chapter discussed how the revolution in military affairs (RMA) changed the face of warfare and the application of military strategy. He foresees a merging of Eastern and Western military cultures as an unforeseen consequence.

2) "The New Revolution in Military Affairs and Changes in Strategic Thinking" by Li Jijun. He is a professor and assists doctoral students in their study of strategy. He is a retired PLA Lieutenant General. One of China's most well-known historians and strategists, Li's chapter stressed the need for serious work to develop China's high-technology weapons.

3) "Discourse on Armed Forces Informationization Building and Information Warfare Building" by Dai Qingmin. He is an Army Major General and a former head of an unspecified

department in the headquarters of the General Staff of the PLA. Since he writes often on information warfare topics, it is assumed that he was the head of the IW Department. Dai's chapter discussed the strategic position of IW and information age attack and defense capabilities.

4) "Taking War to the Air and China's Air Force" by Liu Yazhou, Qiao Liang and Wang Xiangsui. Liu is a Lieutenant General in the Air Force and a very prominent writer. Qiao is a Senior Colonel in the Political Department of the Air Force. Along with Wang, also a Senior Colonel in the Political Department of the Air Force, Qiao wrote the book Unrestricted Warfare that gained great notoriety in the West as an example of Chinese military thinking. The book stated that all methods (nuclear, chemical, etc.) were acceptable in warfare today. Liu, Qiao, and Wang's chapter discusses the primary place of the offensive in modern combat and the important role of the Chinese Air Force in fulfilling that requirement.

5) "The Development of the New World Revolution in Military Affairs and its Strategic Influence" by Wang Baocun. He is a Major General (retired) and expert on both RMA and IW topics in foreign countries. Wang's chapter discusses steps to transform a mechanized force into an informationized force via the RMA.

6) "The Extent and Depth of the Worldwide Revolution in Military Affairs" by Wang Pufeng. He is a former director of the PLA's Academy of Military Science's Strategy Research Department. A Major General (retired), he authored two chapters in the book. The first was on the IW aspect of the RMA, and the second was on the US strategy of preemption.

7) "The 'New' in the New Revolution in Military Affairs" by Tong Weibing. He is an army Lieutenant Colonel (retired) who wrote on the Internet under the pseudonym of the Old Staff Officer. He has established a "strategist" website. Tong's chapter discusses how information and ideas are used to win wars and influence populations.

8) "A Few Thoughts on Advancing Military Informationization Building" by Ma Yaxi. He is a Major and staff officer at the General Staff. An author of several books, his chapter was on the necessity of improving information warfare capabilities in order to meet the challenges of the RMA and thereby win the initiative in future wars. Ma served as an assistant chief editor of this volume.

9) "Fully Calculating the Costs and Profits of War" by Qiao Liang and Wang Xiangsui, previously mentioned with Chapter Four above.

10) "Reviewing US 'Strike First' Strategy" by Wang Pufeng, who also wrote Chapter Six.

11) "The Media in Modern Warfare" by Xie Xizhang. He is the Chief Editor of the Beijing Daily—Literature and Arts Weekly. His chapter discusses the growing role of the media in information war. Xie was an assistant chief editor of On the Chinese Revolution in Military Affairs.

12) "Trends in the Development of World Warfare—Reducing Destructive Force" by Shen Weiguang. Shen is sometimes called the Chinese father of IW. He has written extensively on IW

topics since 1985, and he has published numerous books and articles on the subject. His chapter discusses, not unexpectedly, how IW is reducing the destructive force of warfare. According to Shen, this is important if countries are to keep warfare within bounds as this ultimately could have an effect on the destiny of humans. Shen also served as the chief editor for On the Chinese Revolution in Military Affairs.

13) “China’s Advancing the New Revolution in Military Affairs” by Wu Chenguang. He is a correspondent for Nanfang Weekend. His chapter discusses PLA problems associated with moving from a mechanized to an informationized force.

How Do These Experts Define a Revolution in Military Affairs?

People’s Liberation Army (PLA) analysts have used the term RMA in their works since the mid-1990s. Wu Chenguang wrote that the first time a high-ranking Chinese Communist Party official used the phrase RMA was in 2002 at the 16th National Congress of the Communist Party of China (CPC) by Jiang Zemin. In March 2003 Jiang stated publicly that the RMA must have Chinese characteristics.[\[257\]](#) However, as will be noted below, there is no common understanding of the RMA with Chinese characteristics. Each author quoted has a slightly different comprehension of the term.

Li Bingyan wrote in his chapter in On the Chinese Revolution in Military Affairs that the characteristics of a period of revolution are declining stability and increasing uncertainty in the military field, increasing the value of chance, and eliminating neutrality which allows both extremes to coexist. Li feels an RMA changes the face of war, and it changes the application of military strategy.[\[258\]](#) Li added that a successful RMA requires the ability to clearly see the future as it unfolds, to move toward one’s own strategic objectives, to control new strategic spaces, to maintain great flexibility and elasticity, and to move toward innovative ideas. Victory in war is nothing more than victory in military construction and building.[\[259\]](#) Li added that if military reconnaissance is thought to be the beginning of war, then we have been in a blurred war and peace situation ever since satellites were put up.[\[260\]](#)

Li divided military systems into action systems (attack, mobile, defensive, and support strengths) and cognitive systems (information collection, transmission, processing, and man/machine integration systems). Most important, Li stated that *the current RMA is really a cognition system revolution*.[\[261\]](#)

Li noted that cognition is a major reason why people/soldiers are often unprepared for an attack. There are a host of factors that can influence analysis and judgment: limited foresight, slackened vigilance due to repeated false intelligence from the enemy, complicated warnings, indecisiveness, impact of new technology that isn’t understood, conservative ideas; prejudice; self-deception; pursuing a certain political intention with the wrong policy, bungling attack opportunities, and finding difficulty in deciding whether to keep within limits or to accept a challenge and fight. Also of cognitive significance is the issue of surprise which may be utilized on battlefields in terms of time, space, technology, or methods with the latter two as the primary ways to implement RMA-type surprise.[\[262\]](#)

Li stated that the RMA is not so much a revolution as a military innovation mechanism. It involves absorbing a new philosophical spirit, and it is a new phase in epistemology and methodology. Change gradually arises from uncertainty and it must be regulated.[263]

Li noted that an RMA is a new phase in military strategy research. Further, a successful RMA requires the development of asymmetric thinking, and it must support future asymmetric operations. It must create asymmetry on the battlefield using asymmetry in military scientific research.[264]

Wang Baocun offered another RMA definition. He defined the RMA as

A process of shifting from an industrial society toward an information society as its fundamental cause; with the rapid development of high technology, especially information technology, as its direct driving force; with information as its ‘genes;’ with improving information capabilities as its basic objective; and with ‘systems integration’ as its primary method that is changing the mechanized military patterns of the industrial age into informationized military patterns of the information age.[265]

Wang stated that high-technology warfare has five characteristics: a high degree of control, a movement from electronic warfare to information warfare, a greater role for information dominance, greater prominence for precision attack, and a shorter period of duration. Wang noted that an informationized armed force would have a six dimensional capability: ground, sea, air, space, information, and perception. Li would undoubtedly agree with perception since it is a cognitive factor. This RMA will be finished when there has been a revolutionary change to a country’s military organizational system, according to Wang.[266]

Wang believes US forces used the RMA to set up a complete system of informationized weaponry to include a comprehensive strategic-level, campaign-level, and tactical-level electronic information system. The RMA has also caused theorists to develop innovative warfare and operations concepts (such as IW, network-centric warfare, etc.), established a four-step mechanism for producing combat strength (suggest operations ideas; develop new equipment; carry out tests and exercises; and utilize them in warfare), and practiced virtual warfare in order to accelerate military informationization building. China’s military, Wang noted, needs just such an innovative operational style.[267]

Li Jijun noted that an RMA is not the same as either military reform or a revolution in military technology (RMT). Military reform is a gradual adjustment, and an RMT is limited to weaponry. An RMA involves a series of changes to military theory, methods of operations, weaponry, systems organization, command organization, and so on.[268] China’s industrial RMA was complete only after the appearance of People’s War, which included guerrilla warfare theory and practice. A necessary component of the RMA is countercontrol measures for high-technology warfare. There must be a conventional, asymmetric warfare method of operation that has nuclear equivalent deterrence measures according to Li.[269]

Wang Pufeng wrote that an RMA is a complete change in military systems. Presently, the

worldwide RMA is a very systematic RMA that was initiated after a group of super technologies entered the military arena. The RMA includes a new kind of nature in warfare, a new form of warfare, a new method of operation, a new warfare theory, and a new organizational structure for warfare.[\[270\]](#)

Further, Wang Pufeng believes, an RMA has three elements: military technology and weaponry (material base of the RMA); organizational structure and authorized strength of the armed services (reflections of the achievements of the RMA); and military theory, strategy, and tactics (the innovation aspect of the RMA, or the soul of the effort). These elements are interrelated. In addition, the information-age RMA greatly affects command and control. This is because the revolution has produced automated command or C4ISR systems with a global information grid (GIG), opened up a new field of struggle (the C4ISR confrontation on the networked battlefield and in the domain of computers), and created new kinds of special operations to sow confusion into systems or to destroy them.[\[271\]](#)

Author Tong Weibing added that China's goal in carrying out a new RMA is to keep war within limits: it is not to promote war. Actual strength in modern warfare does not refer to numbers of tanks but to the measures to control information and to paralyze information in war. This is a revolution in the whole military architecture and system of operations. Supporting Li's idea of the importance of cognition, Tong stated that the key point of a transformation is the innovation of ideas. The US military continuously carries out reforms in the areas of ideas, systems, and technology.[\[272\]](#)

What Is Strategy?

Li Bingyan wrote that strategy is a special way of one side's decision makers using information to influence or control the direction of an opponent's decision making activities.[\[273\]](#) It is the wisdom, intelligence, and intellect of decision makers put into a plan in competitive activities. It is the way decision makers gain the upper hand in a competitive environment by calculating the future, grasping the situation, making comprehensive plans, and seeking gains while avoiding harm.[\[274\]](#)

Li wrote that military strategy should absorb the new methodologies, such as systematology, cybernetics, synergetics, mutationism, information theory, dispersion theory, function theory, intelligence theory, optimality theory, homology theory, and fuzzy theory.[\[275\]](#) If absorbed and understood properly strategy will not only be updated but able to take advantage of contemporary conditions.

According to Li Chinese thinking tries to entice the opponent to adopt the strategy that will lead China to the greatest gains. In this sense risk and opportunity coexist.[\[276\]](#) Fighting in the physical, information, and perception realms leaves a wide space for the application of strategy. How strategy is used must change, however, and its capabilities must improve.[\[277\]](#)

Li wrote that the fog of war is used to execute, conceal, and develop strategy. Strategists hope to know the situation on the other side so that their use of strategy and concealment can add to the opponent's fog of war. Planning and designing strategy calls for knowing the enemy while implementing strategy requires that you use a channel of information to send the things you want the

opponent to know.[278]

To thwart the enemy's plans, friendly forces must analyze the size of the interests and contradictions of the two sides. One should arrange factors and see if one's own interest objectives can be realized by influencing or destroying the opponents' cognition systems or by changing the opponent's decision making.[279]

Li added that Western game theory can be characterized as "no matter what game the opponent uses, the game we use must assure the greatest gains and the least losses, that is, the so-called 'maximum/minimum principle'." It is a "connotative solving method" that resolves a contradiction within the contradiction. Game theory is called the algorithm method, and it can be expressed in precise mathematics. It strives for certainty and reliability. Strategy attempts to make the opponent commit errors in the realization of one's own goals. It is a "denotative solving method" in that it resolves a contradiction outside of the contradiction.[280] The new strategic culture must learn to use rules such as international law and maritime law to their advantage.[281]

Li added that the development of IW is a low-to-high escalating development process. US battlefield IW is still using only data and understanding. It cuts off an opponent's flow of information and assures information flows for its side. It will move toward the knowledge layer or knowledge warfare. It will lift information dominance to decision making dominance.[282]

How Does the RMA Impact Strategy?

Li Bingyan stated that high-technology warfare has hastened the appearance of many new characteristics of military strategy. As a result, Eastern strategy must shed some old thinking and take into account six new features:

- Methods are new.
- Information is abundant.
- Content is vast.
- Summaries are strong.
- Preplanning is detailed.
- Resolution is quick.

This implies that the RMA is changing a commander's concept of time, space, and strategy. Military theory can now emerge from the labs, and military strategy can be previewed in the labs.[283]

As examples of strategies and technologies, Li asked how a weak country could fight a technologically superior opponent? Using the comparison of a weak mouse operating against a huge cat, he asked "How could a mouse hang a bell around a cat's neck?" His answer: "Entice the cat to put on the bell himself (that is, make the cat hang the bell around his own neck)." In similar fashion, with regard to a strategy of making a technical opponent do something they don't want to do, he asked the following: "How do you make a cat eat a hot pepper?" His answer was as follows: "You can stuff it down his throat (the most difficult), you can put the pepper in cheese and

make him swallow it, or you can grind the pepper up and spread it on his back. The latter method makes the cat lick itself and receive the satisfaction of cleaning up the hot pepper.”[\[284\]](#) The cat is oblivious to the end goal. This is strategy.

General Dai, discussing the importance of using RMA-generated information as strategies, stated that

Today we should grasp the historical opportunity afforded by making these transformations in this information age and establish the position of methods of IW, especially the “assassin’s blade” method from IW for strategic campaigns, and elevate it to the level of a strategy and lend it a sufficient degree of emphasis, make it a focal point of development, and formulate an effective threat and IW combat capability as soon as possible, thereby gaining the strategic initiative in the military struggles of this new century and even in international struggles.[\[285\]](#)

What Is IW, and How Does It Relate to the RMA and Strategy?

Li Bingyan defined IW differently than most IW specialists, stating that it is the use of information networks or informationized weapons to attack an enemy’s cognition systems. Cognition systems include knowledge systems plus belief systems. Knowledge systems refer to decision making systems built to understand or observe verifiable phenomena and to change the phenomena into perceivable reality. Belief systems refer to systems that carry out guidance for testable empirical information and for information and awareness that cannot be tested or is difficult to test. The patterns of guidance are restricted by the cultural traditions of the people.[\[286\]](#)

Information (and therefore cognitive) supremacy allows for what Li terms “control power.” One must prevent the enemy from understanding your information while knowing everything about the enemy’s situation. Strategy both needs information supremacy and influences information supremacy. While information dominance can allow unidirectional transparency on the battlefield, the side with information inferiority can also send information it wants the superior side to know. Using strategy to control an opponent is creating information misdirection[\[287\]](#) and is increasingly an issue both sides must contend with on today’s battlefield.

Wang Pufeng added to Li’s cognitive focus. He wrote that the most important reflection of the RMA is the extension and expansion of the functioning of human thought by which it makes the release of energy more precise, more scientific, more rational, richer in organization, and more effective. This is intrinsically different from the pure expansion of power.[\[288\]](#)

Li warned that one couldn’t follow rules established by the US (as forerunner) of a concept such as IW. China must guard against strategic misdirection. The real phase of the RMA is informationization, and it is a double-edged sword. It can improve operational efficacy but must adhere to the principles of autonomy and controllability at the same time. Without autonomy there is no initiative.[\[289\]](#) Warfare has crossed the informationization threshold according to Li and concepts such as values, real space, superior and inferior, and benefit and harm have changed.

[\[290\]](#)

Dai Qingmin described IW in a different way, focusing on systems rather than cognition. He defined IW as an effective method to attack combat systems supported by information systems to bring about their complete destruction. This is the basic characteristic that differentiates the construction of military informationization from the construction of national informationization. IW is controllable, cost-effectiveness, and represents the developmental needs of advanced combat strength. IW is not only an aide to tactical combat activities, Dai notes, but an important campaign activity. It can appear separately from tactical campaigns of pure firepower. Information is important for the efficient circulation of energy on the informationized battlefield. Interestingly, in his chapter Dai never once referred to the RMA. However his chapter focused on two important Chinese RMA aspects: informationization and new organizational constructs.[\[291\]](#)

Finally, Wang Pufeng noted that the RMA of the information age is different from past RMAs because it is manifested in the reduction of power and in an increase in precision.[\[292\]](#) By advancing military informationization building with the goal of improving IW capabilities, it is possible to meet the challenges of the new RMA and to adapt to the requirements of informationized warfare and thereby win the initiative in future wars.[\[293\]](#)

IW Will Reduce Destruction

The crux of complete victory is making both warring sides, especially the offensive side, know the outcome without fighting. If it is already known beforehand that war will be detrimental to both sides, then there is a chance that both sides will mutually make concessions and stop the war. This happened at Dayton in the 1990s.[\[294\]](#)

Li Bingyan believes that, with the advances of the RMA, future war should try to reduce destruction. Even Sun Tsu said that the ultimate goals of war are peace and growth and that destruction is not a necessary channel for reaching the goals of war.[\[295\]](#) Perfect war will be war in which neither enemy nor friendly sides have casualties. This will direct attention to weapons such as magnetic kill weapons.[\[296\]](#) IW expert Shen Weiguang suggested “ideal warfare” as a concept and referred to a large number of conflicts between countries in the not-too-distant future that could be controlled early by using simulated warfare to resolve them.[\[297\]](#) The Chinese admired the Dayton Talks that allowed the war in the former Yugoslavia to end based on simulations.

RMA advances will also impact on the conduct of war. People should effectively restrict both the political and military objectives of war. RMA advances in the IW sphere remold ideas on the use of violence. Noncontact war, IW, asymmetrical war, and nonlinear operations can help control the enemy’s use of combat power.[\[298\]](#) Chief targets should be computer network systems that connect the country’s politics, economy, military and all of society. If the destructive effect of war is reduced, then attacks on the spirit of the enemy can be increased. Attacking the spirit will be based on the enemy’s rational knowledge and will be renewable.[\[299\]](#)

IW will gradually evolve into the primary form of war, and military objectives will shift from eliminating the enemy and preserving oneself to controlling the enemy and preserving oneself.[\[300\]](#) The development of weapons has a restrictive effect on the destructive force of warfare. The

forms of war are strategic IW, precision attack, leadership warfare (warfare with reduced destructive force will attack leaders and their purposes using direct measures, pushing leaders to the front of war), virtual warfare (network confrontation, network influence like in the Dayton talks, online campaigns, etc.), and incapacitation (nonlethal) warfare.[\[301\]](#)

IW is tangible war moving toward intangible war. To transform the PLA's force, China must enhance research and planning and study how to win a war with reduced force and how to prevent the destructive force of warfare from escalating. Informationization must play a leading role in reforms, and there must be an increased long-distance precision attack capability.[\[302\]](#) IW may even replace simple firepower warfare. Informationized weaponry forms a system and includes all kinds: of guided-projectile missiles, torpedoes, and other informationized ammunition; of informationized-operations platforms that connect to the networked battlefield; of microprocessor-based individual soldier equipment; and of C4ISR systems, GIG systems, and programmed digital weapons such as viruses, hacker technologies, and so on.[\[303\]](#) The RMA has reduced the number of people per square kilometer on the battlefield while the area occupied by each person has increased.

IW Transforms the Military

General Dai, on the other hand, focuses more on IW's destructive power. He notes that the purpose of a military transformation in the information age is to utilize modern scientific information technology to reform the army; to elevate the ability of the military to develop, utilize, and control information resources; and to comprehensively raise the army's combat effectiveness, enabling the military to have the ability to acquire both deterrent and real-combat capabilities. This requires the construction of information systems, the informationization of weapons and equipment, and the construction of IW theory.

There are fundamental differences in the construction of a military informationization plan from a national informationization plan. These differences are in strategic environments, strategic goals, strategic focal points, and strategic avenues.[\[304\]](#) Thus military strategy differs from national strategy as a result.

Military informationization building refers to the process of using information technology to carry out a complete transformation of the basic elements that make up the armed forces, to optimize information operations capabilities, and ultimately to build an informationized military. Its main tasks include bringing forth new ideas in military theories and operational thinking, improving military organizational structure, bringing about informationization of weapons, and training informationized personnel.[\[305\]](#)

IW's Technological Impact

Wang Baocun noted that an RMA-based, informationized military has two components: military sensing and military communications. The former has increased the surveillance distance of platforms by 5-times and the amount of information surveyed by 25-times. The latter helps ensure unimpeded command, attack, and damage evaluation information, and assists in surveillance, intelligence, tracking, and fire control. This enables an overall synthesis of effort.[\[306\]](#) Thus the technological impact of the RMA on the PLA is expected to significantly increase its military capabilities.

Wu Chenguang notes that Chinese General Xiong Guangkai believes the essence of the new RMA is a reflection of the informationization revolution in the military field. The US military, Wu states, believes that the combat effectiveness ratio of a digitized armed force is one to four over a mechanized force. A military training information network that links the whole military together has already tentatively been activated.[\[307\]](#)

Control of the frontlines by the rear lines is becoming a new trend in warfare thanks to informationized forces. Drones circling over Afghanistan can be controlled from stateside.[\[308\]](#) Liu, Qiao, and Wang note that the war in Afghanistan was the first appearance of drone airborne warfare. The air is where China can win limited war under informationized conditions. Air attack forces have a high degree of controllability, are able to select targets and attack methods, and their intensity is based on the war and operational objectives. This is not just the air force, but the army and navy air assets as well—the joint air attack force.[\[309\]](#)

IW Imparts an Offensive Nature to Modern Conflicts

Ma, like Dai, stresses the offensive. IO with electronic warfare and network warfare as its key contents stresses that an offensive nature is an intrinsic, essential requirement. Only by actively taking the initiative and attacking and by carrying out omnidirectional interference and suppression of the enemy's command, control, communications, and reconnaissance systems will the enemy be rendered unable to fend for itself.[\[310\]](#) It is the RMA that enables this strategic application of the IW tool.

China must avoid being passive in future wars. Developing countries must enhance the construction of information operations forces, particularly assault forces. EW and network warfare are the main methods of information attack. They are the core and the mainstay of IO. Presently the electronic warfare forces of the US military is 2.6% of its total, and the electronic warfare forces of the Russian military is 3% of its total. Compared to this the electronic warfare forces of the Chinese military is too small and must be increased.[\[311\]](#)

Wang Baocun notes that China views the information infrastructures and systems of militaries of even developed countries as still somewhat weak. Therefore, the “trump cards” of the Information Age (as distinct from the nuclear trump cards of the Industrial Age) are: computer viruses; hackers; and high-power electronic-interference units, passive-interference units, high-energy non-nuclear electro-magnetic pulse bombs, antisatellite weapons, and other offensive information warfare weapons.[\[312\]](#)

General Dai noted that information attacks not only destroy forces, but they can also lead to significant financial, transportation, electronic messaging, and electric system shortcomings that can inflict political, economic, and moral harm. IW attacks can paralyze command and control and produce “unbalanced combat.” IW is an “assassin's blade” that is strategic, offensive, targeted, extraordinarily effective, and threatening. As Dai notes, IW/IO is not just a military weapon. Further,

Methods of IW represent the fundamental trend of the development of offensive weapons in the information age. Selecting the construction of IW as the strategic focal point in the

construction of the informationization of the military is a necessary demand to accommodate the development of combat in this age and the urgent conditions of military combat.[313]

How Did the RMA Influence US Actions in Iraq?

Chinese analysts were surprised, Li Bingyan wrote, over the extent of the US's RMA achievements witnessed during the fight for Iraq. They overestimated Saddam Hussein's strategy, and they were fooled by the information the US let out publicly. The US, Li adds, used Sun Tzu to balk the enemy's plans and avoid direct confrontation with the Iraqi military. The Art of War deeply affected what the US and British militaries did on the battlefield. What the Chinese saw was the integration of Western technology and indirect Eastern strategy. "Win without fighting" was discussed, and it appeared that Western militaries were changing from On War to the Art of War. Clausewitz used Hegel's dialectic and Newton's mechanics to analyze war. It is representative of western-strength type military theory. The Art of War uses an Eastern method of dialectic thought, exploring the rules of war and bringing up rich and intriguing thoughts on strategy. It reflects the requirements for warfare in an information society. The US military also is trying to use strategy together with their RMA achievements to overcome Iraq's military strength according to Li.[314]

Before the war started, strategic planning developed on three levels. They are the political and diplomatic level, using morality to attack injustice; the mind, such as psychological attacks and IW; and operations, or carrying out planned destruction and placing target selection, evaluation, and reevaluation at the heart of strategy.[315] Sun Tzu said that the victorious strategist only seeks battle after the victory has been won. Victory first includes knowing fires, calculating first, and preparing first. Making preparations, fighting with the assurance of weaponry, and conducting scientific decision making helps ensure this.[316]

The US military turned the war into a live telecast which was more like a strategic cognitive event. It limited the main points of attack to military targets according to Tong. This outcome made the common man in Iraq feel the "benevolent" side of war. People were less likely to turn against US forces. Iraq was a generation behind the US in technology and concepts and this is the main reason that the Iraqi military ultimately lost.[317]

Xie stated that media warfare included two important aspects in regard to Iraq. Internally, the country's people must be won over to support the war, the legal system must be on board, and the morale of the troops must be inspired. Externally, alliances must be won, and a joint battlefield must be established. The opponent must be isolated, bogged down in injustice, and demonized. The media became an instrument for the government to win public opinion. It also played the role of a "morale bomb" for the military. Media warfare now includes intelligence warfare (that is, use of the media to gain intelligence) as a part of total warfare.

US operational measures with the media included threatening (decapitation, etc.), kidnapping, and blocking (using force to suppress an opponent's voices). The Gulf War of 1991 was easier for the US media because there was only one voice. In 2003 there were competing media voices from the Arab world, and in this war Iraq was not the invader.[318] The US began a broadcast offensive starting in December 2002 that used five different frequencies inside Iraq to persuade Iraqi soldiers to stop supporting Saddam. It also called on the Iraqi military not to attack

allied British and US forces' aircraft. A total of 480,000 leaflets were distributed with broadcast times and frequencies. Operational plans were leaked as well which sent a strong psychological shock to soldiers and civilians alike.[\[319\]](#)

There were different motives at work in Iraq according to Qiao Liang and Wang Xiangsui. US President George Bush wanted to lay a foundation for his reelection: Secretary of Defense Rumsfeld wanted to use the war to promote lightening reforms in the US military: and General Franks wanted to prove that the Army still had an irreplaceable role in modern warfare. The best example of maximizing results in the war was not the use of the air force but bribing Iraqi generals. It was much less expensive.

Other countries should learn from the US and not only about advanced military technology and methods of operation. They should also learn that before each war is fought it is necessary to fully calculate one's own costs and benefits, and not to fight a war in which there is no way to reap profits.[\[320\]](#)

What Is Decision Making?

Strategy is the core of decision making, and information is the material of decision making.[\[321\]](#)

Information that computers produce is greater than the information they process. Because of this, the distance between strategists and the battlefield is also expanding at the same time. In just this way, the next move in the US military's RMA will be to try to carry forward information dominance into decision making dominance.[\[322\]](#)

Li Bingyan defines decision making as a process of information gathering, processing, working, and producing. It can be simplified as reconnaissance, analysis, judgment, determination, and deployment. Obviously RMA-designed forces assist in each of these missions. To move from information gathering to military action requires obtaining, processing, confirming, and transforming information into action. The information formulation chain is developed from data, understanding, knowledge (analysis and evaluation), and wisdom, with the latter being the most important for decision makers.[\[323\]](#) Li added that wisdom is people's ability to understand, analyze, judge, and produce creative thought. Intelligence is the ability to use information to realize a certain goal or objective in various environments. Intellect is the ability to understand a matter and use knowledge and experience to solve problems.[\[324\]](#)

Conclusions

Prominent US Chinese scholars Bates Gill and Lonnie Henley, writing about the Chinese RMA in 1996, noted that China might approximate an RMA reflecting Chinese needs and characteristics in the next 15 years (or by the year 2010). Gill noted that China's self-reliant economic tradition, its Soviet and Maoist legacy, and decentralization of decision making would make RMA progress slow. But, he added, the Chinese had already begun the debate on the RMA shortly after the 1991 Gulf War. They recognized that opportunities for exploitation and potential applications were growing rapidly. And China's leaders understood that its large population offered the chance for significant advances quickly. Economic and socio-cultural factors however may determine how quickly China can adapt to the RMA.[\[325\]](#) China will have to measure its

economic capability to initiate an RMA as well as whether there are enough trained personnel to institute it.

Henley added that even if China could not achieve an information-based RMA in the foreseeable future, this

Does not necessarily mean the Chinese cannot achieve an RMA. It is possible they will make significant breakthroughs in some other direction entirely. In fact, this could do more to shift the military balance in their favor than either of the more conventional alternatives. We would be much more likely to recognize, understand, and cope with a Chinese RMA if it followed the same path we were already on; and less likely to deal effectively with an RMA based on concepts and approaches that are unfamiliar to us...China will not achieve any major breakthrough in the innovative application of technology to military operations...for at least the next quarter century.[\[326\]](#)

There is an implied warning in Dr. Henley's interesting analysis. If China makes an RMA breakthrough in a direction unfamiliar to us, how will we know? How will we recognize "unfamiliar concepts?" Perhaps our recognition will come via books such as The Chinese Revolution in Military Affairs for in such volumes we find ideas and concepts foreign to our mostly information-based technological RMA approach. As General Dai pointed out

If we go our own path to develop military theory, weapons and equipment, and systems of authorized strength we will develop something never seen before in places that no one has ever thought of before; others will be unable to anticipate or resist our "self-accommodating systems;" that way, our military systems will be even more flexible, acquire even more survival vitality and competitive capabilities.[\[327\]](#)

From a military theory vantage point what was most striking about the work under consideration? To this author it was, first, the idea of offering to foreign competitors ideas they will "be unable to anticipate or resist." Li Bingyan was the best representative of this purely Chinese way of thought (How do you hang a bell around a cat's neck? How do you make a cat eat a hot pepper?) that US analysts often do not explore. A second point is how the RMA is changing the application of strategy. Chinese theorists foresee new phases in military strategic research focused on developing strategies to deceive or influence not only decision makers but also large military systems. Strategy now, under the auspices of virtual preparation, "emerges from the laboratories" and must be studied as a military strategic engineering topic. Further, since the RMA changes our conceptualization of time and space and how the two interact, this opens up a command and control revolution with all its strategic implications.

Another striking RMA conclusion of the book is that IW imparts an offensive nature to modern conflicts. Authors noted that not only are offensive operations cheaper in contemporary times, but they are also a way to gain and keep the initiative in a world where wars are short and much more intense and precise. Time and initiative are intertwined with strategy and the offensive.

China's emphasis on strategy is closely integrated with another popular Chinese RMA topic—the cognitive factor. Strategy's core issue is fooling an opponent's decision makers. One

Chinese theorist felt the heart of the RMA was a cognition system revolution and that this was the key to gaining control of the future. Another author believed that a sizeable proportion of future war will be conducted in aerospace, information space, and perception space (that is, the cognitive factor). Intellectualized warfare thus is an important component of this cognitive confrontation. Closely related to cognition is media warfare.

Many of the authors in this book, and several in related articles, have highlighted the concept of innovation. This creative noun may be the term most familiar to Chinese RMA readers as it appears often in RMA articles. It was the subjective application of creativity (innovation?) to objective conditions that Peng and Yao referred to as the essence of the Chinese concept of strategy. Wang Baocun, who unlike Henley firmly believes China can produce an information-based force, wrote that China's military "urgently needs an innovative operational style."[\[328\]](#) Wang also summed up his thoughts on the RMA better than other authors of this book.

First, Wang noted that China must establish a "world military outlook." This outlook includes a world strategy outlook, a world war outlook, and a world national defense and military development outlook. In other words, Wang suggests taking a comprehensive view of world affairs. China's military must move in the direction of integration based on the world strategic situation and China's strategic interests in order to plan and realize China's national defense and military strategies.[\[329\]](#)

Second, Wang noted that a revolution in military thought should focus on information warfare, information awareness, and information construction. Layers of command must be reduced, organizations diversified according to operational missions, and armed forces structures established. In military education this requires giving priority to IW exercises, offering IW and information technology courses, and training people in IW systems and technology. The final goal is to assemble many military systems into one large military system. This requires early warning detection systems, command automation systems, and precision firepower attack systems seamlessly linked. Systems integration thinking must be built into the training process.[\[330\]](#)

Finally, Wang noted that China must learn to use a virtual-practice methodology suited to the new RMA developments. All of this requires innovative operational concepts, theories, and military technology if combat effectiveness is to be quickly shaped and applied. Laboratory exercises will be particularly valuable.[\[331\]](#)

The Chinese specialists who participated in On the Chinese Revolution in Military Affairs clearly believe that the RMA is a revolution of an entire military architecture—its theory, organization/construction, and application—much like the US analysts of the 1990s predicted. But the manner in which it is understood through the prism of Chinese military culture has produced some conclusions that differ radically from those a US counterpart might develop, especially with regard to the RMA's impact on strategy. China's RMA focus is on ideas as much as technology, such as what constitutes a benefit or harm and how the superior and inferior interact.

China may indeed be on the verge of fielding "unfamiliar concepts" as their RMA research unfolds. The concepts appear to be information-based. The US must consider this fact seriously as it prepares its forces for the coming years. China has made these changes much faster than the US

expected, which means the US must be a quick study of the “RMA with Chinese Characteristics” if it is to understand where the PLA is headed in the next few decades.

CHAPTER FOUR: CHINA'S IW-STRATEGY/STRATAGEM LINK

This chapter is a reprint from Dragon Bytes. It addresses the issue of strategy and IW from 1999 through 2003.[\[332\]](#)

Introduction

Stratagems have historically been a key component of China's military culture. They are found in almost every aspect of Chinese military thought, to include command and control and information war. A Chinese PLA Officer's Handbook offered the best definitions of stratagem from a purely military viewpoint for purposes of this chapter. The handbook defined two related concepts: the science of military stratagem and military stratagem. The science of military stratagem is

Both related to and distinguished from strategic science, campaign science, and tactical science. Strategic science, campaign science, and tactical science research problems related to either the full scope or specific aspects of war; however, the science of military stratagem researches problems related to the creation and application of stratagem that cut across all three of these sciences. Strategic science, campaign science, and tactical science research the general principles of war guidance; however, the science of military stratagem researches how to flexibly apply these general principles in war. If the former's research focuses on the "positive path," then the latter focuses on the "deceptive (or scheming) path"; if the former's research focuses on the "constant," then the latter focuses on the "variable..."[\[333\]](#)

Military stratagem was defined in the following way:

Stratagem generally refers to scheming and military strategy (or tactics—taolue); the war planning (or scheme, plot—mohua) employed by the two opposing combatants to be used at different levels of military strategy, military campaign, and military tactics in order to obtain victory. Military stratagem is a product of the development of war, the concrete manifestation of human subjective actions upon material forces. It reflects the general principles of military struggles, possessing a corresponding stable nature and vigorous liveliness.[\[334\]](#)

There is mention of stratagems in many Chinese military articles. In a 2000 article in the Chinese journal China Military Science, authors Major General Niu Li, Colonel Li Jiangzou, and Major Xu Dehui (all of the Communications and Command Institute) defined IW stratagems as "schemes and methods devised and used by commanders and commanding bodies to seize and maintain information supremacy on the basis of using clever methods to prevail at a relatively small cost in IW."[\[335\]](#) The 1992 book Thirty-Six Stratagems offered another definition, noting that

Yin and Yang are two complementary qualities in the universe and everything in the world is

thought to belong to one or the other. Yin, the female element, is associated with the dark and hidden while Yang, the male element, is associated with light and openness. The ancient Chinese regarded ploys and stratagems often hatched and carried out in secrecy, to belong to the Yin. Yin in the Book of Changes is represented by the hexagram for earth which is composed of six lines, with each line broken into segments, resulting in two columns of six short lines, whose product is thirty-six.[336]

Chinese-English dictionaries referenced for this chapter used the words “plan, scheme, astuteness, resourcefulness, strategy, plot, and trickery” most often as an equivalent for stratagem. Thus there is some common understanding of a stratagem from a Chinese viewpoint. The word is understood to imply some measure of scheming, trickery, or deception.

The US Armed Forces does not recognize stratagem as part of its military philosophy. The US Department of Defense’s Dictionary of Military Terms, Joint Publication (JP) 1-02, does not define the term. It does define strategy and tactics. The former is defined as “the art and science of developing and employing instruments of national power in a synchronized and integrated fashion to achieve theater, national, and/or multinational objectives.” Tactics are defined as “the employment of units in combat. The ordered arrangement and maneuver of units in relation to each other and/or to the enemy in order to use their full potentialities.”[337]

The term stratagem is not absent from the English language, of course. One US dictionary defined a stratagem as “a maneuver to deceive or outwit an enemy in war. It is a device for obtaining advantage; trick.”[338] Strategy is defined as “the science and art of conducting a military campaign on a broad scale: distinguished from tactics. The use of stratagem or artifice, as in business or politics. A plan or technique for achieving some end.”[339] Tactics are defined as “the science and art of military and naval evolutions; especially, the art of handling troops in the presence of the enemy or for immediate objectives; distinguished from strategy. Any maneuvering or adroit management to gain an objective.”[340] This indicates that the US understanding of the term also is related to trickery and deception.

Still, it is difficult to capture the overall essence of a stratagem and what it implies to Chinese theorists who use the term. Dr. William Whitson, an American who has studied the Chinese for many years, offered an interpretation of a stratagem from what might be termed an overarching perspective of a Chinese specialist with years of experience in the field of military studies:

I have never seen a Western term that adequately expresses what it means. Westerners don’t understand the essence of the concept. They seek oversimplified words like ‘deception’ or ‘disinformation.’ The practitioner of mou lue zhan starts from the premise that he is engaged not in destroying the enemy physically but in confusing him mentally, hopefully so confusing the enemy that he will become paralyzed. The idea is based on a deeper philosophical idea that any situation is not objectively real. It is instead a projection of many perceptions, especially the perception of leaders. So the focus of mou lue zhan is an enemy leader’s perception. . .it might be translated as ‘attitude warfare’ or ‘perception warfare.’ In effect, military strategy itself and the deployment of troops are made subordinate to the overarching stratagem of creating the enemy’s perception. Westerner’s don’t understand it because they

are taught to believe that victory comes to those with things that make the loudest noise and are the most destructive. To the mou lue warrior, such a viewpoint is childish and wasteful. [341]

Dr. Deborah Porter is a Chinese language specialist at the University of Washington. She added a supporting yet slightly different interpretation of the term. In the ancient dictionary Erya, Dr. Porter writes, mou is defined as “heart.” An annotator of the definition commented that “mou” is using the heart to think (in a calculating way). Mou is also defined as the type of thought that assesses the difficulty or easiness of some action. Sixteen synonyms of the term were listed in the Erya dictionary, including to plan, to delimit, to surprise, to search, to investigate, to visit, and to observe (for the purpose of calculation). [342] In the section on “Shi Yan” (explanations of verbal expressions) where mou is defined by itself, the same definition of “relying on the heart to think” is listed but with more commentary: “the heart is [like] the finest of thread; [its ability] to recognize/discern the minutest [details] ensure that there is no object that cannot be penetrated; the heart is the residence of cognition.” [343]

The Chinese word zhan, Dr. Porter adds, was usually used in the context of warfare and had an ancient meaning more to do with the emotion/sensation of fear. In a military context, an understanding of the objective would be how fear is manipulated, created, and taken advantage of—often in tandem with an element of “surprise” in a battle context. It is also understood as a word for trembling, such as a shaking movement as a response to fear. [344]

The term lue is not as ancient as the other two, at least as is recorded in paleographic and dictionary sources, according to Dr. Porter. The initial sense of the term was agricultural. The semantic sense of the term may have evolved to include the sense of plot or ploy. It has nothing to do with battle. The word lue in mou lue zhan refers to the plan/plot and calculations/observations conducted with the object of manipulating (psychologically) opponents’ emotions, especially those associated with fear, Dr. Porter concludes. [345] Thus, with this complicated etymology, it is not surprising that “stratagem” is a concept not entirely understood by Western audiences.

The Chinese are integrating stratagems into their information-age thinking at many levels. For example, the book Command Decision making and Stratagem, published in 1999, took a historical look at China’s tradition of using stratagems. Author Zian Ruyi noted that “historical wars needed stratagems and future high-tech wars also need stratagems even more. We must ... make them more scientific and modern.” [346] Jia Fengshan, writing in Jiefangjun Bao (Liberation Army Daily) in 2003, noted that science and technology boost traditional stratagems to a new level. They can be derived from and applied to not only the human brain but also high-tech means. Jia noted that “some military experts believe that the ‘differences in stratagems’ lie in the ‘differences in technologies’ under high-tech conditions” and that integrating high-tech with stratagems is going to be an inevitable trend in the future. [347]

The term is often used with other concepts. When discussing the term asymmetry, for example, one Chinese theorist chose to mix the term stratagem with the term tactics. Kang Hengzhen, writing in China Military Science in 2002, noted that “12 crafty tactics” demonstrate the abnormal logic that defines asymmetry. Further, asymmetric operations are no longer constrained spatially due to the advent of high-tech (which has information technology as its core). Traditional

fighting space has changed. Now ground forces must be prepared to consider the effect of satellites that spy on their every move as well as the opponent's ground forces. It is necessary to consider the stratagems that fool these satellites.[\[348\]](#)

These constant references to stratagems indicate that they play a key role whether directly or indirectly in the development of Chinese IW theory and practice. This chapter explains how China uses stratagems in conjunction with IW. First, China is studying how to deceive and manipulate the decision making capability of commanders through the integration of IW and stratagems. Second, the Chinese military is studying how stratagems and high-tech equipment work together. For example, Chinese planners are learning how to gather reconnaissance data (obtained from satellites, sensors, etc.) from the battlefield, compare that data with other data stored in computers, and generate computer stratagems for action (similar to the US courses of action) based on this comparison. Third, based on a network analysis highlighting its critical aspects, attack stratagems are tailored to the different characteristics of the network under consideration. And finally, there is the implication that electron packets are capable of being used as stratagems against networks much as forces were used on a battlefield in the past.

The term stratagem is used often by the PLA, and it is a term that Western audiences must come to understand. It utilizes perception management techniques to fool or paralyze enemy forces. Understanding how the PLA interprets the terms also allows better contextual and philosophical understanding by Westerners of Chinese military writings. This chapter explores China's use of both IW strategies and stratagems.

Integrating High-Tech Weaponry with Stratagems

The topic of developing information warfare strategies and tactics has taken center stage as a key discussion point over the past few years. Even former Chinese President Jiang Zemin underscored the strategic task of “developing the strategies and tactics of People's War in the context of high technology” in his report to the 16th CPC National Congress.

Major General Dai Qingmin, director of the PLA's Communication Department of the General Staff (responsible for IW/IO), is one Chinese thinker who has done as Jiang directed. He wrote in the Number 4, 2000 issue of China Military Science that

...new technologies are likely to find material expression in informationalized arms and equipment which will, together with information systems, sound, light, electronics, magnetism, heat, and so on, turn into a carrier of strategies.[\[349\]](#)

Dai's comments imply that China may intend to use electrons as they once used forces. That is, electrons might be used to fulfill the stratagems “kill with a borrowed sword” and “exhaust the enemy at the gate and attack him at your ease.” Electrons might, for example, help destroy another country's information infrastructure or overcome deficiencies in technology just as forces did in the past. A comparable equivalent to this theoretical development in military art would be Russia creating a virtual operational maneuver group (OMG) of electron forces to attack inside a country, maneuvering electrons as forces were once manipulated.

General Dai's article is an important benchmark in PLA military philosophy. First, as the

prior commander of the PLA's Information Warfare Center in Wuhan, General Dai is a very credible and responsible figure, giving his ideas the stamp of official thinking. Second, in the article quoted above, General Dai broke with tradition and advocated an active offensive to gain the initiative and seize information superiority by attacking first. This offensive emphasis contradicts China's military strategy of active defense and indicates new missions for IW forces. Finally, he noted that integrated and joint IO, two subjects rarely discussed by Chinese specialists, gives more scope and purpose to a People's War. Dai's support of stratagem-based activities and the writings of other Chinese analysts on the subject should be closely followed by Western analysts.

Another important article in [China Military Science](#) that should be reviewed is "Planning and Application of Strategies of Information Operations in High-Tech Local Wars." Authors Major General Niu Li (a professor), Colonel Li Jiangzhou (an associate professor), and Major Xu Dehui (a lecturer) at the Communications and Command Institute offered several ways in which stratagems could be applied in the information age.[\[350\]](#)

The authors defined information warfare stratagems as "schemes and methods devised and used by commanders and commanding bodies to seize and maintain information supremacy on the basis of using clever methods to prevail at a relatively small cost in information warfare."[\[351\]](#) According to Niu, Li, and Xu, Orientals and Occidentals view the combination of stratagems and technology in different ways. This is because their military and social cultures, not to mention their economic prosperity, have evolved in different ways which results in different thought processes. The authors noted:

Traditionally, Oriental people emphasize stratagems, and Occidental people emphasize technology...Occidental soldiers would seek technological means when encountering a difficulty, while Oriental soldiers would seek to use stratagems to make up for technological deficiencies without changing the technological conditions. An Oriental soldier's traditional way of thinking is not conducive to technological development, but can still serve as an effective way of seeking survival in a situation of danger.[\[352\]](#)

There is certainly a Western proclivity to look for technological fixes that has long been recognized and critiqued by analysts. A simple check on when the latest US article was written on IW stratagems would most likely turn up empty. Western audiences have underappreciated the less recognized Oriental fix on strategies and perhaps their importance in general. A proper mix of the two is required, it would seem, to ensure that all sides of a situation are properly assessed.

Authors Niu, Li, and Xu believe that stratagems can help China make up for its deficiencies in high-technology based weaponry. Stratagems are not developed in isolation but by combining human qualitative thinking with computer-assisted quantitative calculations. There are reports of Chinese efforts to use computers to generate military stratagems as a battle unfolds in field exercises. In such scenarios, the operations department of a field unit would collect information from sensors, satellites, and other reconnaissance assets, and enter the data into a computer. The computer would generate stratagems from this input for a Chinese commander's consideration. That is, current battlefield information is compared with established models stored in computers, and from this stratagems are generated. US operations personnel, on the other hand, generate

courses of action for their commander's consideration. This is usually done by a combination of map and terrain analysis and knowledge of enemy locations.

The PLA Science and Technology University reportedly has developed an auxiliary decision making system for military operations research. This may be the machine that produces these calculations. The system improves the PLA's simulated operations capability. It should enhance their combat prognosis capability and ability to grasp tactical situations. This is particularly helpful when considering operational factors such as troop strength, firepower, and sea/air control capabilities, and when performing force-on-force exercises on the network.[\[353\]](#)

The Chinese believe that the models stored in computers will standardize responses to the huge number of contingencies and uncertainties on the battlefield. Computers and the human brain interact to develop IW stratagems under these circumstances. As these authors put it, it is necessary to "let stratagems be integrated into the genes of high technology."[\[354\]](#)

One goal of the use of stratagems is to cause enemy commanders to make mistakes by influencing their cognitive elements and system of beliefs. The idea is to force enemy commanders to develop decisions in the direction set by the Chinese side.[\[355\]](#) Another idea is to fool the high-tech systems, such as sensors and satellites, with fake troop movements or locations. In this way enemy commanders are shown a false picture of what is developing which influences the decisions they eventually make.

LTC Liu Aimin, a staff officer in a General Staff Department of the PLA, added to this idea. He wrote that deception warfare is rising quietly on virtual battlefields. By this he means the insertion of simulated information into an enemy's command and control system. This could cause an enemy to mistake what is false for what is true, or it could throw an enemy command and control scheme into chaos. Liu concluded that "virtual reality information network deception will become an important combat measure on the future virtual battlefield."[\[356\]](#)

Cybernetics, information theory, systems theory and futurology, and decision making systems and theories assist this effort. Chinese theorists use these tools to search for critical points and weak spots in an enemy's system, and then they find ways to paralyze the system. To make this work, junctures and areas of interaction between technology and stratagems must be identified. Stratagems must be devised to be compatible with the characteristics of different networks, and they must be used by a system capable of ensuring information acquisition, transmission, and processing. They must control the entire process in a targeted manner that requires an understanding of how an information contest develops in different stages and time periods. Here, Chinese authors place emphasis on attacking first. This is yet another indication that in the information age an active offense may be more important than an active defense.[\[357\]](#)

In the acquisition or preparation phase, stratagems must interfere with, damage or destroy listening and antilisting measures, camouflage and anticamouflage devices, reconnaissance and antireconnaissance measures, and stealth and antistealth measures among other items. Stratagems may be included in information flows to sever channels of communication while keeping friendly flows of information secure. Some of the methods of influencing information flows are to carry out interference and anti-interference efforts, deciphering and antideciphering efforts, and destruction

and antidestruction efforts. Finally, the processing phase requires stratagems that, in addition to the transmission task, include misleading and antimisleading efforts targeting the enemy's information processing system to cause the enemy to make decision making errors.[\[358\]](#)

The basic goal of stratagems is to intimidate, use perception management, and create fictitious objects (such as fake networks and equipment in an information system) as part of a deception plan whose intent is to hide "true reality." The intellectual battle is now more important than contests in bravery, the authors note, and wide-ranging knowledge and superior wisdom, boldness, and scheming ability are required.[\[359\]](#)

A stratagem can be as simple as misleading the enemy by pretending to follow his wishes. If one knows the enemy's intentions, the enemy can be led into a trap.

A contest in information warfare stratagem is usually conducted in a non-contact manner, and contains efforts to create cognitive errors on the part of the enemy and to influence the contents, process, and direction of thinking on the part of the enemy's commanders and relevant personnel for information warfare; the purpose is to make enemy commanders make wrong decisions or even stop fighting, so as to achieve the objectives of information warfare without fighting.[\[360\]](#)

Of course, the actual effectiveness of this strategy would need to be evaluated based on the enemy's perceived awareness of the strategy's intent and subsequent response. Finally, Niu, Li, and Xu offered ten specific stratagems (which read more like methods) that can be applied to IW. These stratagems include:

- (1) **Thought-Directing**—Direct others' thinking in the wrong decision by attacking cognitive and belief systems and force commanders to make errors. Use schemes with regard to enemy doubts and exploit information relays between enemy units and departments.
- (2) **Intimidation through Momentum-Building**—Generate heavy psychological pressure via intimidation by signaling inevitable victory, concentrating forces, and coordinating information networks. This is to be achieved by creating a situation favorable to China and unfavorable to the enemy. Intimidation is to be achieved via momentum building, achieved by enhancing one's own position, situation, and posture while blocking the flow of information to the enemy.
- (3) **Information-based Capability Demonstrations**—Intimidate by demonstrating capabilities, an action that should not appear to be intentional. The right time, occasion, and modality must be chosen to make information believable to the enemy. At the same time, a unit's true strength should not be revealed, and one should be unpredictable, using both true and false information.
- (4) **Prevailing over the Enemy with Extraordinary Means**—Adopt active and effective measures to generate surprise, and use decisive technical equipment and means of information warfare. Develop and hide information warfare "killer weapons."
- (5) **Using Fictitious Objects to Hide the True Picture**—Hide true reality by creating a fictitious reality. Simulate combat forces using high-tech means, to include the creation of nonexistent

objects (such as fictitious networks and information system, as well as fictitious strategic and operational objectives).

(6) **All-Encompassing Deception**—Apply deceptive schemes simultaneously or consecutively according to strategic or operational intentions. Actions taken should be coordinated and corroborated with one another to ensure the enemy will have no suspicion.

(7) **Prevailing over the Enemy with All-round Strength**—Use all means of information warfare to maintain supremacy. Electronic soft attacks (reconnaissance satellite systems, etc.), hard attacks (informationized precision-guidance weapons, strategic bombings), and C3I battlefield control and management must all be present.

(8) **Going with the Flow**—Mislead the enemy by pretending to follow his wishes. Pretend to “go with the flow” by exploiting one’s knowledge of an enemy’s intentions and the detection of enemy moves in order to lead the enemy into a trap.

(9) **Releasing “Viruses” to Muddy the Flows**—Release viruses to contaminate information flows. Using viruses, the authors note, is an important combat operation. A virus attack is “a technical act, which will have to be based on the use of stratagems in order to play an important role in IW.” Stratagems should create a favorable time for releasing viruses. It is important not only to seize opportunities but also to create opportunities, and to “attack first.”

(10) **Controlling the Time Element**—Control of the time element is crucial. Conducting information “inducement,” “deception,” concealment,” and “containment” operations will help achieve the desired amount of control. [\[361\]](#)

In conclusion, the authors noted that “there are many ways of seizing information supremacy and the initiative in IW, and the use of stratagems is one of the most efficient ways.” The goal of the use of stratagems to Niu, Li, and Xu is to force an opponent to refrain from deciding to launch information attacks in order to achieve objectives without direct fighting. The point of these strategies is to create cognitive errors in the enemy; to influence the contents, process, and direction of thinking on the part of enemy commanders; and to create a multidimensional threat with which the enemy must contend.[\[362\]](#)

Focus on Science and Technology, Not Just Strategy

China’s focus on stratagems is a cultural and historical fact. However, some key Chinese theorists recently questioned whether there is too extensive a reliance on stratagems. If stratagems are being stressed at the expense of technology, then perhaps a weakness has emerged in Chinese military thought that must be corrected. As a result some theorists are trying to better harmonize an integration of high-tech with stratagems.

One of the most prominent Chinese theorists to challenge the stratagem-centered approach is Major General Li Bingyan, Senior Editor of the *Liberation Army Daily (Jiefangjun Bao)*. More importantly he is the author of several works on stratagems and is considered a Chinese expert in the field of strategy. In 2002 Li wrote in support of placing more effort on scientific innovation. He also noted that, traditionally, Easterners put more emphasis on strategy, and Westerners put more

emphasis on technology.[363]

Li writes that Western military power cultures see coordination and struggle as mutually incompatible, whereas Chinese culture emphasizes coordination within competition to seek a point of equilibrium between the interests of the two aspects. Chinese strategists pursue a battle of wits instead of relying on force. As a result, victory beyond the battlefield is a reflection of “big system ideology” in Chinese military strategy. All of these elements must remain a part of Chinese military strategy, but another element must be established—the emphasis not only on trickery and stratagems but on technology. Li notes:

While we are the inheritors of our own outstanding cultural tradition, we should be boldly collecting cultural genes from Western military science and its emphasis on technology. We should make traditional strategy merge with modern science and technology and scientific methods, so as to restore the original intent of ‘Sun Tzu strategy.’[364]

In view of Li’s criticism of his system, should Western theorists spend more time on thinking in terms of strategy and the stratagems of warfare? Isn’t it a known fact that Western armies already spend too much time and focus on technology to answer and fix every problem? Wasn’t a focused reliance on technology at the expense of stratagems part of the reason that NATO’s air forces did not hit targets as well as expected during the fight for Kosovo?[365] The answer to all of these questions is obvious and indicates that, indeed, the US should spend more time on developing stratagems.

Chinese authors Niu, Li, and Xu, mentioned above, also touched on the subject of the integration of stratagems and technology. They noted that information acquisition and processing capacities, and a system’s overall anti-interference and survival capacities, will greatly affect the use of information warfare stratagems.[366] Today, China is in an inferior position in regard to other developing countries and their technological capabilities, although their capabilities are quickly rising. Therefore, it may be necessary to defeat superior equipment with inferior equipment until this ratio can be improved. To do this will require a combination of technology and stratagems in order to allow the “all rounded superior” to defeat those superior in equipment only.

Chinese experts recognize that every piece of equipment has vulnerabilities (even high-technology equipment) and that methods must be developed to attack these vulnerabilities. Examples include subjecting night vision devices to intense light or exploiting existing vulnerabilities, such as the Abrams tank’s vulnerability to sand that was exposed during Desert Storm. Likewise, using operational security measures as the Serbs did in Kosovo (not turning on systems, placing mockups where equipment once was located, positioning tanks near other heat sources in villages, etc.) limited the combat effectiveness of high-tech NATO weapons. The most important point is that *man must create these conditions*, according to the Chinese. He must take advantage of enemy errors or force them to happen since man cannot entrust a nation’s destiny only to the errors that the enemy makes. That is why Chinese scientists and theorists must study “methods of operation and performance parameters” in depth.[367]

All these offensive and defensive methods of operation must be based on a thorough

understanding of the operational and technical performance of the enemy's and our own weapons and equipment. . .we must have a thorough knowledge of the enemy's situation, our own situation, and the situation in the battleground. . .we should study, in depth, the weapons and equipment of our enemy in the operation, identify their Achilles' heel, and work out ways to overpower them.[368]

General Dai on IW Strategies

In the same issue that *China Military Science* published Niu, Li, and Xu's article, it also published Major General Dai's article on "Innovating and Developing Views on Information Operations," mentioned earlier in this chapter. Dai defined an information operation as "a series of operations with an information environment as the basic battlefield condition, with military information and an information system as the direct operational target, and with electronic warfare and a computer network war as the principal form." [369] Since these operations are a confrontation of forces and arms as well as a trial of strength focusing on knowledge and strategies, Dai recommended a "focus on strategies."

Dai noted that scientific and technological developments have given strategies a new playing field. A strategy may carry different contents under different technological conditions. Thus, there is room for traditional strategies, but also room for mapping out new strategies using new technological means. Options include new information-confrontation strategies. [370] Overall a good strategy may

Serve as a type of invisible fighting capacity; may make up inadequate material conditions to a certain extent; may narrow a technological or equipment gap between an army and its enemy; and may make up a shortage of information fighting forces or poor information operational means. [371]

Some specific strategies include:

- Jamming or sabotaging an enemy's information or information system
- Sabotaging an enemy's overall information operational structure
- Weakening an enemy's information fighting capacity
- Dispersing enemy forces, arms, and fire while concentrating one's own forces, arms, and fire
- Confusing or diverting an enemy and creating an excellent combat opportunity for oneself
- Diverting an enemy's reconnaissance attempt and making sufficient preparations for itself
- Giving an enemy a false impression and launching a surprise information attack on an enemy at the same time
- Blinding or deafening an enemy with all sorts of false impressions
- Confusing an enemy's mind or disrupting an enemy's thinking
- Making an enemy believe what is true is false and what is false is true
- And making an enemy come up with a wrong judgment or take a wrong action. [372]

Dai also emphasized that future operations must be integrated, this time meaning to include the use of military and civilian information fighting forces. Information systems are offering more modes for people to take part in IO and offer people a chance to serve as a major auxiliary information fighting force in a future information war.[373]

According to Dai the attainment of information superiority (General Dai used the term information superiority thirty-two times in this article and the term information control, which Dr. Shen used so often, eleven times) is crucial to the utilization of these strategies in a People's War. This will require several steps. First, General Dai noted that professional forces (probably the PLA) would obtain, transmit, and process war information, and jam or sabotage enemy information or information systems. Nonprofessional forces (possibly the reserves) would protect specific targets and injure the effective fighting strength of the enemy. Second, electronic-warfare means (designed to sabotage information gathering and transmission) should be integrated with network-warfare means (designed to sabotage information processing and utilization). Third "soft and hard"[374] forces and offensive and defensive operations should be used. Offensive operations consist of electronic, network, and other units that are used to destroy enemy electronic systems. Defensive operations consist of telecommunications, technical reconnaissance, radar, and other units. The fourth and final step is the employment of an all-dimensional operation that includes integrated and joint operations of ground, sea, air, and space activities. [375]

General Dai remarked that compared to traditional air, ground, and naval operations, to actively contend with an enemy for information superiority, the Chinese need to "establish such a view for information operations as 'active offense.'" The subsequent China White Paper that stressed China's adherence to an active defense posture contradicts this viewpoint. However, Dai's position does support Shen's proposition that China needed an "offensive-based defense," and Dai added that for defense to be positive it must be an "active offensive defense." A negative information defense is one that is passive. This word game may be designed to keep the "information active offense" in line with the White Paper. Dai recommended the active model of resistance used in Kosovo by Serbian forces against the coalition instead of the passive model of resistance used by Iraq during the 1991 Gulf War.

Dai added that stratagems can be used to formulate a strategy before launching or fighting a war, to serve as a sharp sword that sabotages and weakens a superior enemy while protecting or enhancing its own fighting capacity, to serve as a type of invisible fighting capacity, and to evade combat with a stronger enemy.[376] Dai stated that new developments had created challenges to some traditional strategies while promoting excellent conditions for others. He did not specify which strategies he had in mind. However, if defeating strong forces with weak forces in future IW is a goal that stratagems can support or supplement, then stratagems may be one of China's asymmetric means to combat US high technology.[377] In this sense, stratagems would be one of the "magic weapons" that the Chinese are always stressing.

In summary, the August 2000 article by General Dai in China Military Science may represent one of the most important IW articles written in China in the past three years. These thoughts included his reference to electronics as a potential carrier of strategies; the requirement for an active offense in IW; and the need in China for an integrated network-electronic warfare (INEW) concept. The INEW concept is a close equivalent to the US "network centric warfare" concept.

Many of his thoughts in 2000 were later reflected in 2002 in the China White Paper.

Further Thoughts on Stratagems

As mentioned above, Jia Fengshan wrote in 2003 that there is a “growing incorporation between science and technology on the one hand and traditional military stratagems on the other.” He continued that “this trend will not only provide war conductors with new material means by which to work out their strategies, but also make the elevation of the traditional stratagems to a brand new level possible.”^[378] Information technologies such as computers, man-made satellites, and optical fiber communications have created more room for commanders to work out stratagems.^[379] Military strategists working on stratagems must take high-tech factors into account, as it could lead to a boost in fighting capacity. Technical means possess the ability to take the enemy by surprise. Due to the ever-increasing application and integration of high-tech with stratagems commanders must change “their way of thinking, renew their knowledge, and improve their capability to master automatic command systems.”^[380]

In a February 2002 issue of China Military Science author Kang Hengzhen, a Senior Colonel and research fellow at General Staff Headquarters, discussed asymmetry. He defined it as “abnormal logic bringing together two sides that are pitted one against the other. It radiates the dialectic with 12 crafty tactics.”^[381] Asymmetrical thinking includes understanding the nature and attributes of the other party, plus their needs and capabilities. This thinking is “hidden in China’s active defense, and it has become a complete system of theories about preparing for war, strategic defense, strategic counterattack and offense, and so on.”^[382] High technology with information technology as the core has broken the spatial restraints that confined asymmetrical operations in the past, according to Kang. Characteristics of asymmetrical operations are their uncertain objectives, time of use, location, and means of employment. Finally, the author noted that those who can fight asymmetrical wars are those with superior scientific-technological strength and those with superior art of command.^[383]

Another way that the information age (not mentioned in Dai’s article except tangentially, when he noted that information systems and electronics could be carriers of strategies) might affect China’s selection of a form of warfare is whether China can find ways to apply electrons to the thirty-six stratagems of war. Some three hundred years ago, an unknown scholar decided to collect all of China’s thirty-six stratagems and write them down. His work was called The Secret Art of War: The 36 Stratagems. The work emphasized deception as a military art that can achieve military objectives. In the information age, which is characterized by anonymous attacks and uncertainty (for example, virus attacks or the existence of backdoors in programs, making anyone feel vulnerable), the stratagems might acquire an electronic identity that is used to fool or deceive. It should be easier to deceive or inflict perception management injuries (“guidance injuries” according to some translations of Chinese writings) as a result. Thus, the information age is developing into the age of anonymous persuaders and manipulators.

Some argue that in today’s high-tech world, these ancient stratagems are no longer applicable. However, a look at just the first five stratagems demonstrates that this is not the case. Stratagem One is “fool the emperor to cross the sea.” This means that in order to lower an enemy’s guard you must act in the open while hiding your true intentions under the guise of common, daily activities. The IW application would be to use regular e-mail services or business links over the

Internet to mask the insertion of malicious code or viruses. Stratagem Two is “Besiege Wei to rescue Zhao.” This means that when the enemy is too strong to attack directly, then attack something he holds dear. The IW application is that if you can’t hit someone with nuclear weapons due to the catastrophic effects on your own country, then attack the servers and nets responsible for Western financial, power, political and other systems stability with electrons. Stratagem Three is “Kill with a borrowed sword.” This means that when you do not have the means to attack your enemy directly, then attack using the strength of another. The IW application is simple—send your viruses or malicious code through a surrogate or another country. Stratagem Four is “Await the exhausted enemy at your ease.” This means that it is an advantage to choose the time and place for battle. Encourage your enemy to expend his energy in futile quests while you conserve your strength. When he is exhausted and confused, you attack with energy and purpose. The IW application here is to use the People’s War theory to send out multiple attacks while saving the significant attack for the time when all of the West’s computer emergency response teams (CERT) are engaged. Finally Stratagem Five is “Loot a burning house.” This means that when a country is beset by internal conflicts, then it will be unable to deal with an outside threat. The IW application is to put hackers inside the West (under the guise of a student or business) and attack from the inside. While chaos reigns, steal from information resource bases.

Interestingly enough, in Chapter Two it was noted by Dr. Shen that “people have come up with 36 ways to disrupt the Internet and 36 ways to defend against such disruption.” Is it possible that Shen was referring to the thirty-six stratagems of war? Most Chinese will probably think of the thirty-six stratagems since this magic number is a classic ingredient of Chinese numerology, which remains a major part of modern Chinese rhetoric.

Finally, as mentioned earlier, information technology is the core and foundation of the military revolution according to many Chinese military theorists. Invisible forces must be considered in calculating the correlation of forces today. These forces include computing capabilities, to include capacity, communications capacity/volume, system reliability, and the increasing competency and ability of reconnaissance systems to foresee situations.^[384] Each of these elements could be victims of a manipulation stratagem and consequently affect the perception of the user of the system in question. That is, an information strategy can be employed against adversaries by toying with a side’s information infrastructure’s capacity, capabilities, and reliability, all of which are crucial elements in maintaining infrastructure stability. Since information technology possesses global reach, speed of light transmission due to the Internet, and comprehensive integration, the use of stratagems against information infrastructures can have immediate and perhaps long-lasting consequences.

Psychological Manipulation

In its essence, a stratagem is about out-thinking the opponent, forcing the enemy to believe something that is not true. The idea is to manipulate an opponent into a decision or into a movement that is advantageous to friendly forces. Thus stratagems have a significant psychological aspect. Knowledge war also includes the development of superior strategies based on superior knowledge.

Future war may be characterized by chessboard type competition. High-tech knowledge embedded into the circuitry of weaponry will be “directed by master’s degree holders,

commanded by university students, and conducted by experts.” In addition the speed of turning knowledge into weapons will increase as will network competence, automation and real-time systems of early warning, reconnaissance, control and guidance, and attack. This will enable weapons to automatically conduct analysis, and differentiate and identify targets. People and weaponry that are more technologically competent will enable military systems to replace “quantity and scale” with “quality and effectiveness.”[\[385\]](#) Such advantages will give friendly forces a significant psychological advantage as well.

CHAPTER FIVE: DIRECT INFORMATION WARFARE

This chapter summarizes three of four chapters from Major General (retired) Dai Qingmin's book Direct Information Warfare, 2002.[386]

Introduction

Future war will be fought between or among high-tech systems if current trends continue. An important Chinese work explaining the new information-age battlefield concepts on which these systems are based is the 2002 book Direct Information Warfare. The book's author is General Dai Qingmin, who served as head of the Chinese General Staff's Communication Department and thus is assumed to have served as the head of IW as well for the Chinese General Staff. The book's focus is network forces and network warfare.

Defining Terms

Dai defines a host of terms in his description of "direct IW." Among others, these terms include information warfare, network warfare, strategic network warfare, computer network space, computer network attack, digitized armed forces, network security, network psychological warfare, information operations, and integrated network-electronic warfare. This chapter begins with a listing of key terms found in Direct Information Warfare. They provide an excellent overview of Chinese theory and understanding of information-related concepts in 2002:

Battlefield Information Environment. This environment is described as the general designation of the various information and information systems pertaining to the battlefield, its periphery, and its operations. It is the information space in which two warring sides carry out information operation activities. It has expanded from tangible geographical space to virtual information space. It is primarily made up of three basic elements: electromagnetic-spectrum information space, computer-network information space, and psychological information space.[387]

Campaign for Capturing Information Supremacy. This type of campaign is represented by the sum of a series of mutually connected actions that include electromagnetic attack, network attack, psychological attack, and firepower destruction carried out in a joint campaign battlefield space and time using information operation forces. It is based on electronic warfare and network warfare and pertinent army, navy, air force, and second artillery operational forces arrayed against the enemy's campaign and strategic information systems that hold together his operational systems. The IO campaign is developed for the purpose of capturing information supremacy.[388]

Computer Network Attack (CNA): The various measures and actions taken to make use of security flaws in the enemy's computer network systems to steal, modify, fabricate, or destroy information and to reduce or destroy network utility.[389]

Computer Network Space (CNS): This is a physical space that actually exists. Civilians call it bit space, and the military calls it the bit battlefield. Thus it may be limited to a building or cover

an entire war zone. It is now an important component of military power. It mainly includes six elements: computers, communication networks, software, information, network users, and network infrastructure. It also has four functions: a communication function, a database storage function, an information processing and control function, and an information services function. Computers are the key part of networks, and they are used for the functions of information entry, transmission, processing, and control.[\[390\]](#)

Digitized Armed Force (DAF): This is an armed force that is supported by computers, uses a digital technology network with digital communications technology, and provides individual soldiers, commanders, and various combat support and support systems with the capabilities to collect, transmit, and process battlefield information.[\[391\]](#)

Information Operations (IO): This is the general designation for the various operational activities and measures carried out to weaken or destroy the useful efficacy of the enemy's information systems on the battlefield, to include ensuring that one's own information systems retain their efficacy. It is an important component in joint operations. It stands side-by-side with firepower and mechanized power as a third attack measure, and it is also the prerequisite and the basis for capturing the battlefield initiative. These operational measures have designated operational goals, operational objectives, and operational forms.[\[392\]](#)

Information Operations Theory. This is a rational understanding of the essence of IO. It is a high-level summarization of the laws of IO, the guiding rules of IO, and the force construction and rules of use for IO. The theory of IO has three parts—technical theory (special technical aspects), fundamental theory (general laws), and applied theory. The latter explains the special laws for the various specific practices of IO and provides the theory for the direct foundation for IO. Applied branch theories include electronic warfare, computer network warfare, and psychological warfare.[\[393\]](#)

Information Supremacy. This term refers to controlling the dominant position in battlefield information within the scope of a particular time and space. It consists primarily of the right to access information, the right to transmit information, the right to process information, and the right to use information. It means having the rights of freedom and initiative when using information and controlling battlefield information initiative within certain space-time limits.[\[394\]](#)

Information Warfare (IW): This term refers to the use of computer network systems to gain enemy intelligence and destroy enemy systems in order to improve the military's defense and attack capabilities as well as the intelligence capabilities of one's own side. Applications include attacking the enemy's "nervous system" with viruses and various long-range control measures, paralyzing the computer network system of enemy headquarters, or entering wrong intelligence and wrong commands into the enemy's military command system, thereby enabling the goal of victory in war.[\[395\]](#)

Integrated Network-Electronic Warfare (INEW): This is the composite use of the two measures of electronic warfare and network warfare on the informationized battlefield. It consists of adopting a series of operational actions to destroy the enemy's networked battlefield information systems and ensuring the normal operations of the networked battlefield information

systems of one's own side. Its goal is to seize battlefield information supremacy.[\[396\]](#)

Network Psychological Warfare (NPW): This is an operational activity that uses the theory of psychology, has computer networks as its carrier, and uses measures such as psychological propaganda, psychological deception, and psychological deterrence to break down the spirit of the enemy's military and people...NPW will certainly play an even greater role in future wars and will exhibit extraordinary power.[\[397\]](#)

Network Security (NS): This is the use of various computer, network, encryption, and information security techniques to protect the secrecy, integrity, and authenticity of the information transmitted, exchanged, and stored on public communication networks. These techniques have the capability to control the dissemination and content of information.[\[398\]](#)

Network Warfare (NW): This is any kind of information attack or defense operation that is carried out on the entire network space and that has computers and computer networks as the main targets and advanced information technology as the basic measures. Types of network warfare include attacks (penetration, obstruction, and dismemberment) and defense. There are two battlefronts: strategic network warfare based on the Internet and battlefield-network warfare based on battlefield networks. NW is intellectual warfare that highlights competition between knowledge and algorithms.[\[399\]](#)

Psychological Information Space. This is the information-dependent space that is composed of the numerous actions and organizations that fight against the understanding, sentiments, and wills of battlefield commanders and troops. For example, news media, nongovernmental organizations, unauthorized parties, intelligence organizations, and so on are all considered part of this space.[\[400\]](#)

Psychological Supremacy. This is the ability to change the will of the adversary and influence his motives by influencing the way he looks at all that is going on around him and the causes of things.[\[401\]](#)

Strategic Network Warfare (SNW): This is a kind of indirect operational measure based on the Internet. It can be initiated in peacetime or in wartime.[\[402\]](#)

Direct IW Concepts

Dai wrote about several information-related topics in Direct Information Warfare. Those highlighted in *italics* are based on their relevancy and interest to a US IO audience. They are information operations, information supremacy, networks, network-warfare units and personnel, network psychological warfare, IO mobilization, and INEW. Each is discussed separately below.

Information Operations

Dai states that information operations are soft-kill measures designed to make an enemy force lose effectiveness, conduct faulty decision making, and institute ineffective command measures. Effective IO will create imbalances in enemy force coordination and limit its control of weapon systems. IO has specially designated operational goals, objectives, forms, and measures.

IO's features are its inclusiveness (from start to end of an operation) and ability to conduct operations in the rear areas of enemy forces. Flexible methods of operation include deception, confusion, deterrence, and other measures such as electromagnetic-jamming suppression, computer-network attacks, and comprehensive firepower destruction.[403] Dai notes that soft weapons cover the ears, block the eyes, and kill the nerves and can include feints, bluffs, and harassing attacks to cause confusion. Hard weapons, on the other hand, sever the arms, hinder the legs, and destroy the body. They include new concept weapons such as electromagnetic-pulse bombs, directed-energy weapons, carbon-fiber bombs, and other new IO weapons. A final information measure is the use of Special Forces to airdrop on and infiltrate into a region and jam or destroy nodes and crucial targets of an enemy's information system.[404]

Information operations are a combat force multiplier in that they are devoted to getting the greatest results with the least investment. This is especially true for joint operations that use IW techniques. Battlefield space, operational areas (electromagnetism, psychology, computer networks, social sciences), and operational actions (offense, defense, mobilization, support) are all "omnidirectional" in joint operations.[405]

Electronic camouflage is known as the magician of the informationized battlefield according to Dai. Electronic camouflage uses electromagnetic and thermal technological measures to simulate and duplicate the environment and make friendly targets blend in with their background. This "hides what is true" and "displays what is false" about the target. It can help thwart enemy electronic attacks and protect one's own systems. Metal foil strips, angular radar reflectors, colored smoke screens, plasma, multifrequency-electromagnetic screens, photochromatic coatings, and optical bait are examples of such measures. Smoke camouflage now includes smoke made up of metallic chemical compounds and plasma which, when mixed with certain polymers in specific ratios, make smoke screens that can fluctuate to be consistent with the target and its background.[406]

The 1999 conflict between NATO and the Federal Republic of Yugoslavia is viewed as a type of IO defensive case study according to Dai. He refers to this operation often to describe how various information defensive measures offset NATO's asymmetric offensive advantage. Lessons learned include concealing to the greatest degree information radiated from one's own information systems, controlling radiation, using deception and camouflage, and hiding signals among other measures. Radar operators had to learn how to confront the following NATO threats: reconnaissance jamming; attack by antiradiation weapons; attack by stealth aircraft and missiles; and penetration by ground and air defense missiles and aircraft. "Active defense" and "offensive defense" are two operational measures Dai recommends to confront these threats. If the "offensive defense" is used, targets must be attacked in some order of priority, attack measures must be rationally selected, and the correct opportunity to attack must be chosen.[407]

Dai believes that the essence of IO is intelligence warfare and strategic warfare under high-technology conditions yet IO will, like past operations, include specific stratagem use. "Making appearances, creating circumstances, using spies, and balking the enemy's plans" will be included in the struggle for information dominance. Indirect tactics imply the use of strategies to "appear where the enemy is not expecting you," "make changes the enemy cannot understand," and "make appearances" (the best way to avoid reconnaissance is not being invisible but creating false

appearances). Science, diversity, and multiple channels of information are needed to convince someone that what is false is true. Lures must be used to make people take the bait. One must seize, create, and control opportunities to fight. To work, these soft measures must be combined with hard weapons.[\[408\]](#)

The idea of combining subjective guidance (creativity) with asymmetric operations was explored further by Dai. He writes

On the informationized battlefield, the side that is in the inferior position carries out asymmetric operations mainly by giving full rein to the subjective dynamic effects of operational guidance and the comprehensive efficacy of other factors for gaining the upper hand, by exploring asymmetric postures that are beneficial to one's own side, by checking the strengths of the opponent, by exposing and enlarging his weaknesses, and by gaining limited superiorities and initiative...what this form of operations basically touches upon is primarily not satellites, cables, and computers; it is people.[\[409\]](#)

Further, Dai states that to conduct asymmetric information operations requires adherence to certain principles. The first principle is to attach importance to independent operations, which means selecting the time, place, and conditions favorable to one's side. A second principle is to use strengths to attack weaknesses. The third principle is to simultaneously develop all kinds of measures to offset enemy dominance. This was demonstrated in excellent fashion by the Federal Republic of Yugoslavia's use of corrugated iron and smoke to obscure the vision of pilots or to misdirect radar signals generated by incoming attack aircraft and missiles according to Dai.[\[410\]](#)

He points out that there are strategies of blind spots, nodes, weak points, and questionable points (the latter being areas where the enemy has not yet sized up the situation). Another strategy is to create situations that are beneficial to one's own side. This requires that one integrate science and art, strategy and tactics, and enticement and concealment to create an exploitable situation.[\[411\]](#)

People create strategies and Dai notes that the initiative, flexibility, and creativity of people are the real keys that IO personnel must exploit. He states that

Laying all one's hopes on technology is dangerous. The road to future losses may not be from a fall in technology, it may be primarily poor strategy. In reality the informationization of the forms of warfare has opened up an even broader space for playing tricks and using strategy and for using the indirect to gain the upper hand.[\[412\]](#)

Dai stresses that since warfare is showing a "plebification" trend, the emphasis on people's talents and creativity must increase. The populace can now participate to a greater degree than ever before by taking part in network warfare far from the front lines. As a result of their participation, the populace and civilian networks are now subject to attack just like military networks.

Dai not only feels that civilian networks are subject to attack but also that the Internet allows countries to be subject to penetration by different values, ideologies, ways of life, and histories.

The Internet exports culture and serves as a carrier and channel for cultural factors.

Internet actions have produced cries of a digital invasion or the spread of information colonialism from some countries. Dai states, however, that it is US “network frontiers” that have already penetrated into other countries and threatened their “network sovereignty.” China must build its own “digital Great Wall” to keep out such influences he adds.[\[413\]](#)

Information Supremacy

Dai writes that achieving information supremacy is an important part of campaign planning. Campaigns for capturing supremacy will be subcampaigns of joint campaigns and one of the latter’s independent objectives. In campaign operations a series of interrelated IW operations will be carried out on campaign and even on strategic levels, and they will be organically integrated with other operational actions to arrive at the campaign objective of capturing information supremacy.[\[414\]](#)

There are four main actions associated with this action. First is carrying out information harassment and reconnaissance in the form of intelligence warfare, psychological warfare, and military deception among other means. Their main objectives will be to gather intelligence from information systems and networks and to conceal information used in deception, political, and diplomatic struggles. In other words, the goal is to hide the operational intentions of the friendly side.[\[415\]](#)

Second, the subcampaign must focus on carrying out information attacks. It is vital to gain the initiative here. Main targets of attack are the information processing and decision making centers of the enemy. Third, friendly forces must take advantage of blinded radars and paralyzed command structures from subcampaign actions to initiate more firepower and supporting information attacks. These attacks will be targeted at command and control centers, air defense systems, electronic-warfare centers, missile launch positions, and other point targets. In addition to firepower attacks, soft attacks will be conducted using electronic interference, network attacks, antiradiation destruction, and directed-energy weapon attacks. Finally, joint firepower and support-information attacks will take place. Air force, navy, and some long-distance army firepower units will be involved. Supplemental attacks will be organized based on information reconnaissance that determines the degree of destruction imposed on the enemy.[\[416\]](#) Whether Dai’s four-step process will only serve campaign planning and the acquisition of information supremacy or be the manner in which China initiates an information attack in general is not known.

Dai believes that Eastern nations are adept at being resourceful and overcoming obstacles. In such ways, an inferior military, if it controls the commanding height of information supremacy or even a limited portion of it, has a chance to gain military success. There are more chances now to do so since the information field has expanded exponentially. There are reconnaissance satellites, aircraft, ground, and sea stations along with electronic and early-warning aircraft, stealth, antiradiation and radiation weapons, network-warfare equipment, and intelligent radar. These developments further enable the strategic goal of “subduing the enemy without fighting” via information warfare. Whoever controls information supremacy, Dai adds, controls war initiative.[\[417\]](#)

In joint operations under high-tech conditions, in order to achieve information supremacy, a difficult series of steps must be initiated. Each of the two sides must use all capabilities to include information deterrence, information interdiction, information deception, and information contamination. This makes the substance of command and coordination extensive and complicated. [418] Offensive and defensive information warfare actions and systems must be integrated in joint operations. Further, civilian information-warfare forces must be included in army, navy, and air force information warfare forces. [419] The combination of integrated, all-purpose forces will enable supremacy. Dai did not mention any coordinating mechanism for this integrative process.

In addition to the four sub campaign measures for attaining information supremacy in a campaign, Dai visualizes three states in the battle for information supremacy. The initial battle is between information carriers. This period or stage of battle is usually called electronic-information warfare. Since information carriers are becoming harder and harder to attack, the focus is now shifting to a confrontation over information content, Dai writes. A content battle, the second stage, ensures that intellectual information warfare will become the intermediate stage in the development of the battle for information supremacy. Thought-information warfare, the third state, is the highest stage of information warfare because, by directly destroying the thinking of the information users, it is possible to fundamentally destroy the enemy's operational intentions and operational capabilities with the highest efficacy. Such destruction affects the overall war situation. Thought-information warfare will become a reality when biotechnology and information technology are closely tied together. These three stages make up the basic means for developing information supremacy. [420] Thus once again, as he did in the section on IO that emphasized asymmetry and strategy, Dai emphasizes the cognitive aspect of IW.

IW coordination to capture information supremacy includes close coordination between IW and firepower-attack actions, coordination among IW actions of the troops, and coordination between various IW forces and actions. [421] Information supremacy is the commanding height of current and future warfare. Without it, one can lose other supremacies. That is, capturing control depends on information supremacy. Dai added that information supremacy is primarily made up of electromagnetic supremacy, network supremacy, and psychological supremacy. [422]

Networks

Information systems such as networks are the adhesive that link operational elements and forms together. They affect the stability and progress of an operation; require flexibility, mobility, and a tight defense; and need an innovative command system, force structure, operational plan, and thought process. [423]

Network space is composed of bit streams made up of the digits "0" and "1." The power of this bit stream is superior to the power of conventional weapons. This is because bit streams now control, Dai believes, not only the collecting, transmitting, processing, and distributing of information but also operational weapon systems and potentially the thinking of command decision makers and operational personnel. This implies that operational objectives of network space now include the will, feelings, and cognitive processes of an enemy. Network space causes new operational thinking and methods. Further, network space changes the limitations imposed by geography. Traditional boundaries are no longer military boundaries. [424]

Network space and information networks/systems are now of such importance that they are key objects of attack according to Dai. Computers and networks are the main targets, and network warfare will become the main operational form of IW. In this day and age, there is no distinction between peacetime and wartime network warfare. Network attacks could as easily be conducted against telephone networks or gas pipelines (the diversification aspect of network warfare), and they can be covert thus making early warning difficult.[\[425\]](#)

Network warfare (NW) ensures concealment, omnidirectional intrusion, and otherwise unobtainable operational results than if traditional military measures were used. NW has four levels: physical (the computer network's equipment); transmission (signal paths for information); logic (software and data in computer networks); and super-logic (applications that support computer networks and the results that are produced).[\[426\]](#) The expansive nature of integrated operational space allows for more types of operations than currently exist. Strategic, campaign, and tactical centers can be attacked without the problem of creating a large-scale destruction area. Network warfare systems can attack communication hubs, finance centers, and traffic hubs thereby directly influencing the strategic situation and decision makers. These attacks have the potential to paralyze the enemy's political, military, economic, and cultural systems.[\[427\]](#)

However, network warfare could develop in another direction and work to create "network deterrence" or "network containment." That is, it may be more valuable for both sides to simply comply with the rulebook of not attacking one another's networks if two sides attain a mutual balance of network power.[\[428\]](#)

A main focus of computer network war (CNW) is to seize intelligence related to operational objectives. This process is also called computer-network reconnaissance. Software must be developed to help scan online information and to intercept and crack valuable information codes. The latter includes the hardware configuration of the topological structure of all network nodes, communication systems, encryption methods, and network protocols. Data mining and fusion processing tools are valuable as aides to gather information on system platforms, the system capabilities of application software, and the geographical location of target nodes. Reconnaissance can be entirely secretive, or it can be deceptive. The latter includes gaining the trust of the mainframe of the side under observation. Computer network reconnaissance is the prerequisite for seizing victory in warfare. It helps choose opportune moments, places, and measures for attack.[\[429\]](#)

IW represents the integration of network warfare and electronic warfare, and its goal is to achieve information superiority. For example, introducing a computer virus into the C4ISR system of an opponent may become a significant method for the conduct of IW. Network warfare is designed to attack the brain of the enemy's C4ISR system, according to Dai, and this affects strategic decision making and the overall strategic situation. Dai believes that battlefield network warfare (focused on C4ISR) has evolved from hacker warfare. EW attacks the transmission links, and network warfare operations attack the processing links. As a result some believe that whoever has integrated-network and electronic-warfare dominance in system-versus-system confrontations will control future war.[\[430\]](#)

Network Warfare Units and Personnel

Dai believes that network warfare units should look for and infiltrate the network routes to be attacked. This is apparently a peacetime function, for he adds that in time of war, units must be “able to organize and implement virtual reality and virus attack and other network warfare operations under unified plans.”[\[431\]](#) Since these units may affect the war’s overall situation, Dai recommends in wartime putting them under the control of the most senior battlefield command, and in peacetime strategic command organizations should centrally organize them. Network units will lead to new forms of operations and new arms of service. Whoever controls information and controls networks will have the whole world at his feet, according to Dai.[\[432\]](#)

Personnel strength plays a huge role in making key operational decisions about the network and in maintaining the security of network space. For example, network warfare commanders must be very proficient in networks and network technology. They must know what technological measures are feasible to obtain their operational objectives or understand staff suggestions of even better ways of attaining operational intentions.[\[433\]](#) Personnel must have excellent ideological qualities, such as a steadfast political nature and good moral qualities. They must have a desire to succeed and a competitive and innovative nature. Finally, they must have the ability to handle psychological pressure.[\[434\]](#) Other special qualities include a talent for organizational skills, innovative capabilities, and the ability to make forecasts and strategic decisions. Finally, they must be able to flexibly meet contingencies.[\[435\]](#)

There are three basic ways to train network-warfare personnel. These ways are in colleges and universities, in on-the-job training, and in recruiting from among the people since there is such a social context to network warfare. It will be difficult for anyone to differentiate between military and civilian personnel since so much of network warfare is conducted behind closed doors. Dai states that this also means there must be a strong network-warfare reserve force. Reserve forces will play a huge role in hacker attacks and in spreading viruses against enemy countries. He added

The multitudes of netizens around the globe will without a doubt play an important role in future network warfare. Effectively mobilizing and organizing wide-spread netizens and computer personnel to carry out a ‘people’s network war’ will be a magic weapon for gaining the upper hand in network warfare.[\[436\]](#)

Building competent personnel remains the primary task above all other issues. Three kinds of people are needed: high-science and technology experts, resourceful commanders, and professionalized troops. For the most part *these people must understand information offense* according to Dai. This may imply that “network warriors” are under consideration as a new arm of the services as has been suggested by several Chinese authors over the past five or so years.

Network Psychological Warfare

Regarding network warfare in general, Dai notes that the more humankind relies on computer networks to gather information, knowledge, and intelligence, the greater the ability of networks to influence people’s understanding of events. He noted that

Network warfare will also rise from currently being focused on confrontation on the physical level and logic level to confrontation on the super-logic level and that is the level

of perception. The computer field will penetrate deeply into the thought processes of the human brain, influencing the spirit, moral, and consciousness of the adversary, disturbing the adversary's decision making mentality and the direction of decision making, forcing the enemy to give in to our intentions and demands, and forcing the enemy to submit by not fighting or by 'psychological warfare.'[\[437\]](#)

Network Psychological Warfare (NPW) combines traditional psychological-warfare thinking with modern network-information technology. This type of warfare has several characteristics according to Dai. It can transcend the nature of time-space. It cuts across national boundaries (space) and can take place in peacetime or wartime. It can influence people's awareness and feelings in many fields, to include politics, economics, culture, and military affairs via propaganda, intimidation, deception, enticement, bribery, and deterrence. Virtual deception is of particular concern as a network psychological technique. Technology can edit or piece together different visual scenes and environments to create a picture or incident that confuses truth with falsehood. Information can be published under any name and wishes can be displayed in wanton fashion. Most important, NPW is extremely timely. It can take place literally minutes after an event. This can make the substance of the material appear more pertinent, reliable, and effective without the benefit of a proper timeframe to check out the facts. In turn this has the potential to enhance psychological panic or create social chaos.[\[438\]](#)

The goal of NPW is to attack the enemy by way of network media and win victory without fighting or with the least amount of fighting possible. It is a form of psychological warfare. NPW attempts to capture a moral strategic initiative, shake the enemy's will and determination, and make the enemy passive and lose confidence. One of the methods to achieve these aims is to establish special websites for the conduct of psychological warfare and publish all types of deceptive, disturbing, leading and deterring information. The idea is to disrupt normal judgment, block other information channels, and create misconceptions in the enemy.[\[439\]](#)

Dai believes that future fighters will battle for psychological superiority. This will include fights for knowledge, decision making, and command authority. Psychological control, especially of decision making personnel, will become the highest stage of capturing information superiority. Information and psychology cannot be separated. There will develop a repeated confrontation for psychological supremacy, a battle of the consciousness of one side to affect the consciousness of the other side by means of computer networks. NPW's power comes from the Internet's traits of being interactive, open, timely, widespread, diversified, and influential. People's recognition systems are the target. When the media misrepresents their environment it is very difficult for humans to test or verify it in Dai's opinion.[\[440\]](#)

Information Operations Mobilization

A Chinese IO strength seldom discussed in the West is information mobilization. In fact the concept is almost foreign to US audiences in particular. The Western substitute for mobilization is usually associated with the concept of information integration or with a nation's information or cyber-security policies. The Chinese believe that to sustain the IO battlefield the national economy, information infrastructure, information goods, reserve forces, and information technology forces must be mobilized. Dai's discussion of network personnel supports this concept.[\[441\]](#)

Traditional mobilization included the pursuit of quantitative and qualitative superiority in manpower, financial, and material resources. Information mobilization adds superiority in comprehensive information topics (information networks, groups with high intelligence, etc.) to that list. It includes numerous mobilization exercises and can be viewed as an additional deterrent force that fuses technology with comprehensive national strength, forces, and weapons. Mobilization for information operations supports the nation in both peace and war and supports both military and nonmilitary areas. Information mobilization laws and mobilization leadership are under development to guide exercises and to provide well-developed contingencies in case of war.[\[442\]](#)

Integrated Network and Electronic Warfare (INEW)

With regard to INEW, Dai wrote that EW and network warfare are the two main forms of information operations. They cannot be mutually independent but must be comprehensively used and coordinated. INEW shapes battlefield information warfare, Dai added, and it will become the main expressed form of information operations. It can also be called physical IW. Academia divides IW into operational secrecy, military deception, psychological warfare, EW, computer network warfare, and physical destruction. Network warfare and EW, however, are the main means of conducting operational activities.[\[443\]](#)

Dai notes that only through the integration of electronic warfare and computer network warfare will it be possible to master IW. INEW will have as its goal the capture of information supremacy in electromagnetic and network space on the two battlefield trends that have developed, the informationization of weapons systems and the networking of information systems.[\[444\]](#)

Further, INEW's elements are reciprocally complementary and require coordination to bring out the best in each. This is a comprehensive form of operation that integrates command, power, targets, and operational methods with the goal of destroying, controlling, and paralyzing the command and control system of the enemy's military. INEW's focus is the core issue of capturing information supremacy and carrying out omnidirectional information attacks.[\[445\]](#) Operational INEW methods include:

- Interfering and destroying
- Blockading and intimidating
- Luring and pinning down
- Creating false realities and paralysis
- Feigning attacks
- Sowing discord and making suggestions
- Suppressing and overloading
- Impeding information transmission and enemy network utilization
- And capturing the initiative in electromagnetic and network space.[\[446\]](#)

Battlefield transparency will increase with the use of INEW, making the entire information domain a potential space for confrontations. The enemy's strategic, campaign, and tactical centers can be attacked simultaneously.[\[447\]](#)

Dai points out that operational secrecy, military deception, and psychological warfare have been used since ancient times. However, INEW allows them to be fused together in ways never before possible.[\[448\]](#) Dai also called for attacking vital targets to get twice the result with half the effort and to adopt tactical and technological measures to lower the effect of enemy attacks. With regard to the latter point, Dai wrote that multiple methods of flexible resistance should be developed. These include creating net-shaped dispositions, jamming wireless reconnaissance equipment, carrying out reverse tracing and counterdestruction of enemy websites, and creating situations. With regard to the latter point, situations will be created through the integration of science and art, strategy and tactics, and enticement and concealment methodologies.[\[449\]](#)

The Commanding Heights of Future War

In future wars, the focus on the fight for this ‘commanding elevation’ of information supremacy will be more and more complicated, and more and more fierce. Even though a force may be superior, once it has lost this ‘commanding elevation,’ it will still become a ‘blind person,’ a ‘deaf person,’ and a ‘target,’ and it will fall into circumstances of passivity and coming under attack. A military with inferior strength, if it controls this ‘commanding elevation,’ even if it is a limited ‘command elevation,’ will have the possibility of gaining military successes that are not bad.[\[450\]](#)

Dai discusses in some detail the contradictions, forms, nature, methods, and targets of IW. He also focused attention on future war’s major characteristics. Dai stated that there are five “contradictions” in getting to the essence of IW. First, even in the face of so much information, it is difficult to know the enemy. Second, an individual can threaten an entire country in the information age. Further, in some cases the more technologically advanced a country becomes, the more vulnerable it becomes as well. The flood of information is so great today that accurate analysis, evaluation, and synthesis are the most valuable parts in making judgments and decisions. One must ensure that information is not contaminated, since contaminated information will produce nothing of value on the enemy’s intentions. Regarding individuals who threaten to damage a country’s information assets, these individuals are often hard to find or retaliate against. Third, a country can become so dependent on networks that it can suffer great economic and security losses if attacked. Fourth, one can have strategic depth but little security if information systems are not protected. Finally, a military victory does not equate to strategic or political success in the information age.[\[451\]](#)

Dai next comments on the forms, nature, and methods of information warfare. These forms include intelligence warfare, electronic warfare, computer-network warfare, psychological warfare, and virtual warfare. Three of these forms, network war, psychological war, and virtual war, are important due to their unique characteristics. First, computer network personnel can determine the success or failure of a network attack. Such attacks can be totally independent of a nation’s power or its number of troops. CNW can be conducted at any time in different weather conditions or regions of the world. Second, psychological warfare has as its goal the capture and maintenance of battlefield psychological supremacy. Finally virtual warfare is the use of virtual reality and computer imaging technology to manipulate technology (make it appear that enemy commanders are giving speeches against the war), develop virtual air fleets so that the enemy sees false information on satellites or radar, and create virtual battlefields and insert them into the enemy’s command and control system. The use of holographic religious icons is also a possibility

in Dai's opinion.[\[452\]](#)

Dai notes that IW has “five **natures**:” precursory nature (begin before other operations); whole course nature (will run throughout an entire operation); high efficiency nature (get the greatest results with the least investment, maximizes simultaneity of operations); omnidirectional nature (permeates all aspects of campaign operations); and complex nature (multi-element forces take part and operations are diversified). IW is composed of the “two –tions:” diversification and integration.[\[453\]](#)

There are many **methods** of operation in regard to information warfare. Omnidirectional reconnaissance is one such method. In peacetime it is important for reconnaissance work to focus on collecting technical parameters and specific properties of all categories of information weapon systems and electronic information products used for military objectives. Once technical parameters are collected it might be possible, for example, to artificially make gas, fog, and heat products that interfere with the operational parameters of high-tech equipment. During wartime, the focus should be operational mission requirements, collecting battlefield information in a timely manner, reconnoitering troop locations, and establishing an omnidirectional ground, sea, air, space, electromagnetic, and network-information reconnaissance system. Information reconnaissance is growing. It is precise, real-time, and comprehensive. Future war is thought of as the victory of the detector, and this is the role that information reconnaissance will play. Information reconnaissance consists of electronic warfare, radar, radio technology, and network reconnaissance. Reconnaissance platforms include ground, sea, aviation (to include unmanned aircraft), and space platforms (which utilize electronic, photographic, and early warning radar satellites). Dai noted that electronic information systems are the foundation of space systems, making up some 75% of the systems in various satellites and weapons. Like other systems, they are also susceptible to information attacks.[\[454\]](#)

Targets of electronic attack are C4ISR systems, which are like a person's system of perception (or his eyes and brain). Interfering with these systems interferes with intelligence collection and paralyzes command and coordination. Weapons control is lost as well. Once hard kill measures are developed fully, these targets will be destroyed and not merely jammed.[\[455\]](#)

Dai appears to enjoy quoting statistics from the Gulf War as supporting evidence for his focus on information warfare. For example, he notes that in the Gulf War the volume of communications in only 90 days surpassed the volume of 40 years of communications in Europe. That, he notes, is the importance of establishing the right of information control. Grabbing control or obtaining information supremacy must begin before warfare is initiated. The US launched electronic warfare and intelligence warfare more than six months before the war began. Such actions are in line with Sun Tzu's concept that “the clever combatant seeks battle after the victory has been won.”[\[456\]](#)

With regard to future war, Dai notes that a major characteristic of future operations is to destroy an opponent's information control and coordination capabilities. Information attack methods are conducted according to the following priority listing: attack information sources, attack information channels, attack information targets, and attack information equipment. Information defense methods include information counterattack, information protection, and

information restoration. Operational methods include combining the old with the new, the military with the civilian, using the indigenous to attack the foreign, and using the weak to attack the strong. [457] Finally, via network links and nodes, efforts will be made to infiltrate an opponent's networks used for economic and military purposes. Databases will be altered, false orders issued, and computer viruses planted. Political, economic, and military intelligence will be stolen. [458]

Dai's Recommendations/Conclusions

Dai recommended establishing a new national security concept suited to the information age and elevating network-based strategies to the level of the national security plan. He advised speeding the pace of informationization within the country as a whole and speeding the establishment of rules and laws for an information network-based security regime. He added that controlling the initiative in war and destroying the adversary's operational intentions will enable Chinese forces to control the course and development of a war. This must be the operational standard for network warfare forces. [459]

Dai also noted that Chinese theorists have recognized the importance of information operations in periods of peace, competition, conflict, crisis, and war and then from war back down to peace. Reconnaissance monitoring and intelligence collection are very important, as is information warfare in the political, economic, cultural, and media fields. Strategic deterrence, fights for public opinion, economic competition, and political developments are all attempts to achieve information supremacy. Combat now includes the nonmilitary arena as well as the military arena when it comes to information. The line dividing the military from civilians is more blurred than ever before, and the armed forces cannot totally protect the civilian infrastructure as it once did. [460]

Dai's recommended trends for capturing information campaign supremacy include the following:

- Carry out scattered and concealed information harassment and attacks to gather intelligence from systems and networks while concealing ones operational intentions
- Carry out the suppression of enemy information attacks that are focused on key points such as the processing and decision making centers of systems
- Carry out missile firepower and supporting information attacks to take advantage of the confusion caused from disrupting enemy radar signals, interrupting communications, paralyzing command, losing coordination, and losing control of weapons. Simultaneously conduct electronic interference, network attacks, antiradiation destruction, and directed-energy weapons attacks
- Carry out joint firepower and supporting-information attacks on command posts, communication hubs, electronic-warfare centers, guided-missile positions, radar positions, and other targets. [461]

Dai notes that the overall ratio of information operations forces to other forces must be increased and new operational measures developed. In the end, the commanding height on the informationized battlefield will be the attainment of information supremacy and with it battlefield initiative. The latter can be developed fully with subjective guidance and with the establishment of

an asymmetric operational ideology. Information systems are the adhesive that links operational elements and forms operational functions.[462]

Dai's discussion focuses heavily on obtaining key information via reconnaissance of foreign computer systems in peacetime. It is only through reconnaissance that victory in future wars can be assured. As he states, "Computer network reconnaissance (CNR) is the prerequisite for seizing victory in warfare." [463] His focus on CNR provides added context to current Chinese operations aimed at the reconnaissance of US systems. This includes both the Titan Rain attack on US systems and the reconnaissance operation conducted against the US Naval War College.

Of added interest was his focus on network psychological warfare. It is interesting that, like Li Bingyan, Dai focuses on the cognitive aspect of IW more than most senior IW leaders. Not only does he direct the reader's attention to the virtual space that the media and propagandists try to influence but also to the virtual-based command and control decisions that leaders must make. He also focuses attention on the use of stratagems in both defending against high-tech weapons and in manipulating the perceptions of enemy forces. This implies that the will, feelings, and cognitive processes of an enemy are the operational objectives of network space. Network space causes new operational thinking and methods.

Finally, Dai focuses on the power of bit streams (or "0s" and "1s") to control the collection, transmission, processing, and distribution of information and weapon systems and potentially the thinking of command decision makers and operational personnel. Network space changes the limitations imposed by geography. Traditional boundaries are no longer military boundaries.[464]

直面信息战
Direct Information Warfare
Dai Qingmin
2002

Table of Contents

Chief Author: Dai Qingmin
Publisher: National Defense University Publishing House
Date of Publication: 2002

Chapter 1: Approaching Electronic Warfare - "Spears" and "Shields" in the Field of the Electromagnetic Spectrum.....	1
Electronic Warfare—A Leader in High Technology Warfare.....	3
Looking Back 100 Years—Talking about the History of Electronic Warfare.....	8
A Virtual Trial of Strength—Communications Confrontation.....	13
Covering the Eyes—Radar Confrontation.....	19
Chasing Light and Pursuing Electricity—Antiradiation Confrontation.....	25
Electromagnetic Thunderbolts—Opto-electrical Confrontation.....	30
There Is Skill in Concealment—Stealth and Counter-stealth.....	35
Terrifying Waves—Acoustic Confrontation.....	40

The Thunder God's Eye in the Sky - Satellite and Strong Radiation Weapons Confrontation.....	47
---	----

Chapter 2: Click Network Warfare - The New Plane of Subduing the Enemy without Fighting.....	53
Network Warfare Is Rising Abruptly; Have You Made Adequate Preparations?	55
Network Psychological Warfare—Taking Off Your Bridal Veil.....	142
Future Roads—Developmental Trends in Network Warfare.....	147

Chapter 3: An Informal Discussion of Information Warfare.....	155
Gradually Tending Toward Information Warfare that Leads War—an Informal Discussion of the Status and Use of Information Warfare.....	157
The Imperceptible Information Space—the Information Environment of the Information Operations Battlefield.....	163
Informally Talking about the New Characteristics of Information Warfare.....	169
The New Face of the “Five Warfares” of Information.....	179
Information Warfare.....	182
The Methods of Operation of Information Warfare Are Not Suppositional.....	189
Information Supremacy—the “Commanding Elevation” of Informationized Warfare.....	192
On the Informationized Battlefield—Information Warfare Units.....	202
Deception Techniques in Informationized Warfare.....	211
An Equal Number of Antennas and Firearms—Greeting the Age of Information Reconnaissance.....	214
The Magicians of the Informationized Battlefield.....	220
Information Operations Mobilization—the New Form of War Mobilization Under Modern Conditions.....	225
The Essence Is Weapons; the Wise Will Triumph—New Ideas about Information Operations Personnel.....	231
Gaining the Upper Hand by Scientific Theories.....	240
Building a Solid Shield for Information Warfare.....	242
Exploring Information Warfare in the Twenty-first Century.....	248

Chapter 4: Integrated Network and Electronic Warfare—Taking the Pulse of the Information Battlefield of the Future.....	255
The Basic Connotation of “Integrated Network and Electronic Warfare”.....	257
The Basic Characteristics of “Integrated Network and Electronic Warfare”....	261
“Integrated Network and Electronic Warfare” Is the Inevitable Result of the Development of Electronic Warfare and the Sudden Appearance of Network Warfare.....	267
“Integrated Network and Electronic Warfare” Is the Inevitable Product of the Development of Information Operations Theory and Practice to Certain Levels.....	272
The Main Groups and Rules of the Information Battlefield Called Out by the Integration of Networks and Electronics”.....	275
The Trial of Information Strength in Joint Operations.....	279

The Transformation of Dominance on the Information Battlefield..... 289
Paying Close Attention to Campaigns for Seizing Information Supremacy..... 298
Postscript.....304

CHAPTER SIX: DECIPHERING INFORMATION SECURITY

This chapter summarizes several sections from Colonel (retired) Shen Weiguang's book Deciphering Information Security, 2003. [\[465\]](#)

Introduction

Information security is of huge concern to Chinese military and civilian planners. In China, as in the US, millions of dollars have been spent putting firewalls in place and securing networks. Chinese planners are cognizant of the information security problems the US has encountered and realize their implications for Chinese specialists. While aware that they cannot eliminate all of these problems, Chinese planners nonetheless have worked to minimize them and continue to seek creative ways to overcome known and projected deficiencies.

Colonel (retired) Shen Weiguang's Deciphering Information Security provides an incisive look into Chinese methods to thwart information security problems. It examines Chinese planning for the construction of an information security regime. The selected sections under examination here are Shen's lectures and articles on information security and IW issues in 2002 and 2003. Deciphering Information Security also provides a detailed (more than 100 pages) design plan for a Chinese Information Security University. Work on the university was to be completed between 2002-2005 according to Shen, although the location of the university was not specified. Perhaps it is located at Wuhan where other PLA command and control and IW organizations are located. The university has a military security specialty among others.

The various section headings below represent this author's selection of the most important items from a separate lecture or article in the book. The books' Table of Contents is listed at the end of this chapter for easy reference.

10 July 2002, Baoguo Temple, Beijing[\[466\]](#)

The issue of information and network security, which accompanies the development of informationization, and the rise and increasing prominence of information warfare, the form of warfare that is invisible and non-violent, is an issue of technology, but above all else it is an issue of strategy.[\[467\]](#)

In this lecture Shen discusses information security's impact on national security in general. As the quote above indicates, he considers IW to be an issue of technology but warns the reader not to forget that more importantly IW is an issue of strategy, continuing the main theme of Decoding the Virtual Dragon. Shen covers specific aspects of information security such as its technological and cognitive aspects and the impact of holes in information security on politics, economics, culture, and the media.

Shen believes that the old tangibles of national security (borders, etc.) are being replaced by intangibles (information, knowledge, etc.). The concept of "information territory" has extinguished

the overall importance of traditional boundaries. Information territory “is distinguished by the information radiation space of the propagation power and power of influence of a country or a political bloc. Information boundaries are invisible, irregular boundary lines that divide the information territories of all countries or political blocs.” [468] Shen discusses the possibility of “network countries” springing up overnight. The “silification” (use of computer chips to control many aspects) of politics may enable information alliances in the hands of the masses to develop at the expense of national boundaries, regions, and governments. This could lead to the dissolution of traditional countries in Shen’s opinion.[469]

As a result, old concepts must be shed and new ones developed. At the same time, China must avoid appearing weak, and its leaders must move along the pathways that are the most viable for the country. One of the most important strong points that must be developed is information security. It must be made a part of the national security base for any developed country. Further, information warfare and information operations are strong points that must be leveraged along with information security. Technological shortcomings in these areas can affect the security of a nation in the information age and affect the ability of a nation to defend itself.

Shen states that IW is a fight for information supremacy and has at its heart winning without fighting. Forms of IW include electronic warfare, network warfare, psychological warfare, ideological warfare, and media warfare.[470] IW is focused on infrastructures and on leadership. It can destroy or damage both equipment and the mind.

With regard to equipment, strategists examine infrastructures and suggest theories to drive the development of new technologies. Superiority comes from applying the proper thinking about how to use new technologies. Shen believes that military information and network security building are priority developments. It is very difficult to determine who the network opponent is, from where the threat emanates, and whether a war has indeed started or not. Shen asks whether viruses will cause weapons to misfire or navigation systems to malfunction, and whether battlefield information will be encrypted, falsified or fabricated to manipulate an opponent?[471] These developments will impact on the subjective ability of commanders to see through the electronic fog of war as the movement of electrons becomes a permanent fixture on the battlefield. Network reconnaissance, the collection of intelligence, and the impact of such wars on public opinion will all be affected by this change.[472]

Shen warns about cognitive information security as well as technological security. IW attempts to keep an opponent’s strategic and military actions within limits while working to destroy morale. The human factor is more important in the information age than in the agricultural age since human creativity has the potential to cause the destruction of entire economies if properly developed. Shen cites the example of the Cold War. It is an older example of a strategic information war that was very successful for NATO in his opinion and enabled it to overcome the Warsaw Pact, a type of nondestructive war that wouldn’t have been possible in the agricultural age.[473]

Shen has more to say about what damage IW can cause to the mind. He believes that the Internet has assisted in integrating all kinds of information, to include ideology and Eastern and Western cultures, almost without restraint. This is a danger to the information security of the mind

in that “the side that starts out with various goals can use this to shake the other country’s social systems and convictions and spread an opposing ideology.”[\[474\]](#) This is of particular concern because information is the resource that best represents overall national strength according to Shen. If information’s content is manipulated in accordance with the goals and plans of an opposing nation, then moral and spirit decrease as well as the country’s overall national strength. Since Chinese researchers and academicians go to great lengths to compute comprehensive national power or strength, Shen’s concern is understandable.

Holes in information or network security can affect other areas of comprehensive national power such as politics, economics, or military issues. The power to penetrate invisibly into a country’s military, economic, diplomatic, cultural, educational, scientific, and political affairs and to affect a nation’s spirit, psychology, and ideas, can directly influence international events through the use of such information warfare means.[\[475\]](#)

Shen seems particularly impressed with the ability of information to influence political events. He notes that computer networks include newspapers, videos, periodicals, and other media forms that transmit information quickly making politics more transparent and participatory. Of greater concern, he notes, is the ability of networks to establish antigovernment groups, to launch reactionary public opinion propaganda, to pass false information, to alter the contents of information, to carry out spying activities, and to steal national political intelligence. The spread of network technology also allows international political events to influence local political issues. Shen does not, however, ignore the benefits of the Internet such as exerting pressure on decision makers and resolving issues without the intercession of politicians.[\[476\]](#)

Shen foresees a major shift from Clausewitz’s dictum that war is a continuation of politics by other means. Rather he sees the information age as empowering individuals, nonpolitical groups, and other insurgent-type groups:

War is also not merely a continuation of politics, and it is not merely the highest form of struggle between people, countries, classes, and political groups; rather, it has also become a measure for nonpolitical groups and even for individuals who are in pursuit of their own interests to demonstrate their existence. Enterprises, religious groups, terrorist organizations, tribal guerrilla warfare groups, drug trafficking groups, and other criminal gangs can all set a war into motion. The concept of war has undergone a revolutionary change.[\[477\]](#)

In this respect Shen believes that issues other than politics, all inspired and empowered by information technology, will rewrite Clausewitz. Is war now capable of becoming a continuation of criminal/guerrilla/religious/drug activities by other means? Shen notes that countries possess thousands of targets susceptible to attack while terrorists, criminals, and drug organizations, for example, possess relatively few.[\[478\]](#)

Shen devotes as much attention to economics as he does to political and military views. He believes that economic security is the most important element of comprehensive security and that competition is war in the economic sector. To corner a market one must attain a lead in the possession and analysis of information. This will guarantee the ability to assure quality, variety, price, services, and deliveries on time. Again, only information and network security will

guarantee this superiority.[479]

Of somewhat lesser importance, but still vital to a nation's well-being, is the issue of cultural security. Culture is defined by Shen as the bonding agent of a society, the basis for social stability, the provider of social norms for people, and the designer and portrayer of all kinds of social systems. National cohesiveness can only be maintained if equilibrium is maintained between one's culture and the imported culture represented by the information age. The information age can result in values, political views, and images being broadcast in a country that result in damage to relations among races, religions, or even countries. Confused citizens may not be able to separate fact from fiction thereby causing chaos, panic, or fear and affecting a country's political framework and society's security.[480]

The media is of concern when it comes to damaging a country's cultural cohesiveness. Shen is aware of information's power to penetrate into a country and damage the spirit of a country or person. He notes that countries should strengthen the guidance of direct public opinion propaganda, and they should screen, sort, reject (if necessary), or refuse information that is useless or damaging to the nation's or the people's ideological culture. At times, and under specific environmental situations, the government should increase control over the media according to Shen.[481]

To counter information-related political, military, economic, cultural, and media developments, Shen recommends the creation of an information security strategy that reflects the country's traditions and characteristics. There must be goals, tasks, and focal points for both an information defensive and information offensive strategy with the emphasis on the former. This may include the development of information age deterrence forces and their information age weapons. The country's ability to produce information products and technologies directly reflects on China's national strength, making information capabilities a new element of overall strength. A unit of investment in software is more effective than ten units of investment in hardware in Shen's opinion. Those who possess advanced technology thus control the initiative and are restricted only by investment and development in the field of scientific and technological research where the real competition in national strength lies. Cooperation in international security fields also helps to expand stability.

Key technologies to research in Shen's opinion include computer-virus-confrontation weapons, nuclear electromagnetic-pulse weapons, lasers, ion beams, and other opto-electrical beam weapons. He believes national information products must be substituted for foreign parts and equipment. This includes network designs, operating systems, routers, and chips.[482] Further, an "information-security confrontation lab" must be built, a lab that allows confrontations between offensive and defensive systems. Then China can find its problem areas and solve them. The development of intellectual property, simulated research, and innovative research is essential if China does not want to be dependent on someone else's inertia in the information field.[483]

Laws and regulations must also be strengthened in the information-security area. This includes building a solid information-security management system, establishing information-security standards and a classification protection system, building information-defense forces and a unified intelligence system, and enhancing law enforcement contingents assigned to information-security issues.[484]

With regard to training specialists, Shen recommends developing an information security university with Chinese characteristics. This most likely means training that introduces stratagems, INEW, and other Chinese-specific terms and techniques. Training of various types must be afforded to employees of national departments; and government, industry, service organizations, network security industries, businesses, and authentication organizations. This also requires the development of information security as an applied science that studies issues of information, information systems, and information and network-security defense in the field of information application.[\[485\]](#)

Summarizing this speech, Shen notes what must be done in seven steps:

1. Leaders must be responsible and take charge of network security and information building.
2. The military, People's Armed Police, and other departments must defend and counterattack hostile forces and terrorists who take advantage of networks.
3. Macroscopic planning must be developed.
4. Software and hardware must be developed at lower costs and increased efficiency.
5. Defense and offense must be developed simultaneously.
6. Close attention must be paid to publishing information security laws.
7. The propagation and education of public opinion must be enhanced.[\[486\]](#)

August 2002, Baoguo Temple, Beijing[\[487\]](#)

In this speech a month later at the same location, Shen states that information security is the foundation for national security. He expresses concern that IW has dramatically changed the traditional forms of war. IW can use EW, network warfare, intelligence warfare, psychological warfare, hacker warfare, virus warfare, media warfare, and firepower warfare to destroy information installations and attack enemy knowledge and belief systems in unforeseen ways. IW is manifested in deception, isolation, containment, contamination, and guidance (perception management may be what Shen meant by guidance).[\[488\]](#)

Shen notes that the focal point of national security has changed in the time of global informationization. Summarizing his earlier speech he notes that nations must have a strategic understanding of IW because it touches not just the military but all areas of politics, economics, the spirit, and society. Now, information security must be guaranteed to keep economics from becoming chaotic, politics from becoming unstable, the military from losing its efficacy, and culture from losing its direction. A country's strategic objectives now include defending information territory and resources and improving national and social information-security support capabilities. Threats to information security are present in the information infrastructure, its resources and contents, and information management.[\[489\]](#)

To counter these threats Shen recommends the development of information-deterrence forces. Their job is to contend with adversaries, focusing on reconnaissance and other capabilities while paying attention to countercontrol measures, seizing the initiative, and offsetting and controlling the threats of information power from other countries.[\[490\]](#)

Shen recommends the development of a national information security support system. The system appears to be a further refinement of his July comments in the Baoguo Temple. He lists the main tasks of establishing a national information security support system^[491] as follows:

- (1) Set up an information security strategy with Chinese characteristics. The strategy should rationally define strategic developmental objectives and tasks to include what to do and what not to do. There should be emphasis placed on the subjective role of mobilizing the masses to include strategic personnel reserves and emphasis on the utilization of key mental (information security specialists) resources. Building prominence in the areas of spirit and moral is a key point and includes strengthening the guidance of “open public opinion propaganda.” This will help develop and expand Chinese ideological culture. China must counter foreign information, screening and sorting information and rejecting, resisting, and stopping damaging information.
- (2) Enhance the building of a legal system for the information security field. This includes developing the proper system of laws and regulations for China’s information-network security and establishing a national information-security law-support center to study techniques for tracking crimes and gathering evidence.
- (3) Start a national information security infrastructure program. This requires that China promotes domestic production of information-security products and uses technology that China can control such as operating systems, routers, and chips.
- (4) Strengthen information-security evaluation and authentication systems. China needs to develop its own security-evaluation system and to conduct an evaluation of the country’s key information infrastructure and key systems and networks as soon as possible. This includes the four office work resource systems (Golden Customs, Golden Tax, and financial monitoring and management projects) and the eight service system projects (Golden Finance, Golden Shield, Golden Audit, social security, Golden Agriculture, Golden Quality, Golden Water, and the telecommunications related information systems).
- (5) Promote standardized research and application.
- (6) Establish a mechanism for handling emergencies in information security. This includes establishing better monitoring, early warning, and containment of harmful information. In other words, a crisis management system focused on information security. As Shen notes

We should build a national information security crisis handling center, assemble crack troops and capable commanders, be responsible for organizing and coordinating the work of detection, be on guard against counter-control of national information network security and information content security, improve rapid response capabilities, and answer the information security crisis that is confronting China.^[492]

- (7) Formulate a complete set of special policies for implementing these measures as quickly as possible. Shen recommends using market mechanisms to start the industrialized development of information-network-security technologies, products, and services.
- (8) Expand research into information-security conflicts. China must establish a mechanism for simulating information-security conflicts. This will help researchers to

discover, understand, study, and solve problems while enhancing domestic capabilities.

- (9) Enhance information-security training and education. China must build a national information-security education and training center that is responsible for the organization and guidance of training and educational work in the national information security field.

To strengthen the management field, Shen recommended establishing six centers and one agency. The agency would be called the National Information Security Support Management Agency. The centers would be: the National Information Security Center for Supervising Law Enforcement; the National Information Security Evaluation and Authentication Center; the National Information Security Crisis Handling Center; the National Information Security Legal Support Center; the National Information Security Education and Training Center; and the National Information Security Conflict Research Center.[\[493\]](#)

The Information Security University[\[494\]](#)

As mentioned above, Shen also submitted a plan in Deciphering Information Security for an Information Security University. This entry was not dated, so it is assumed that Shen included the university concept as an example of his future intentions.

Shen outlines the university's strategic orientation, its resources and conditions, the policy for running the university, developmental objectives, and other important management activities. Investment expenditures are listed along with the equipment required to run an information-security-technology laboratory and research and development center. Specific information security (IS) departments include: political IS, economic IS, science and technology IS, social IS, international IS, national defense IS, IS technology, IS engineering, IS management, and the national IS department.[\[495\]](#)

With regard to the National Defense Information Security Department, Shen writes that specialties would include national defense and military affairs issues. The department would train specialized personnel who understand IS defense and attack techniques and theory in the military arena. All specialties would emphasize training in military science and practical information attack and defense techniques. After graduation all students should be able to work in national defense and military departments at all levels.[\[496\]](#)

Shen emphasizes that network-information technologies and methods can threaten the political, military, economic, and social order of a country if information security means are not in place. These technologies have no traditional past comparative aspect, so they are unique. Network informationization has thus turned into a struggle between information defense and information attack and is manifested as a struggle for capturing information control.[\[497\]](#) The focus of the university is to learn information-security system as attack and defend means.

Written in February 2002, the plan laid out short-, mid-, and long-term goals. The short-term goal is to establish within one to three years the first common, full-time university in the information-security field and in the country, centered on undergraduate education with supplemental professional training and nondegree education. The mid-term goal is to establish

within three to eight years a domestic university in the information security field with an integrated undergraduate degree education and a graduate master's degree education. The long-term goal is to establish within eight to thirteen years China's first university in the information-security field with integrated bachelors, masters, and doctoral degrees with integrated education, scientific research, and production capabilities. The teacher to student ratio is expected to be about 1:29.[\[498\]](#) Shen noted that the university's policy will be "study for the purpose of application." Six of these teaching plans follow. All of the plans (to include the economic plan) are part of the military information security specialty, demonstrating the attention even the military pays to economic affairs.[\[499\]](#)

Teaching Plans/Course Outlines for Military Information Security Studies[\[500\]](#)

(2-1) Teaching Plan for Fundamental Specialty Courses for Military Information Security

Course Classification	Information Security University Information Security Branch Academy Military Information Security Specialty		Periods/Lab Hours		Credits		Semester Schedule	
	Required Courses (A)	Electives (B)	(A)	(B)	(A)	(B)	(A)	(B)
	Fundamental Military Command Science			20		1		1
Military Command Automation Systems			36		2		1	
An Outline of Information Warfare			36		2		2	
Information Operations Technology Science			36		2		3	
Compiler Language			72/54		4		5	
C Language Program			54/40		3		3	

Fundamental Specialty Courses	Required Courses	Design		
		Periods/Lab Hours	Credits	Semester Schedule
	Data Structures and Algorithms	54/30	3	4
	Information Theory	36	2	5
	Network Principles and Communication	72/40	5	6
	Database Fundamentals and Application	54/30	3	4
	Coding Principles	72/40	4	5
	Operating Systems	54/36	3	4
	Introduction to Codes	72	4	6
	An Introduction to Information Security	20	1	3
	Information Security Laws and Regulations	20	1	3
	Total Number of Credits for Required Fundamental Specialty Courses		35	

(2-2) Teaching Plan for Fundamental Specialty Courses for Military Information Security

Course Classification	Information Security University Information Security Branch Academy Military Information Security Specialty	Periods/Lab Hours		Credits		Semester Schedule	
		(A)	(B)	(A)	(B)	(A)	(B)
Required Courses (A)	Electives (B)						
	Strategics		20		1		2
	Campaign Science		20		1		2
	Tactics		20		1		3
	Military		20		1		3

		Strategy	20	1	3		
		US Military Strategy	20	1	4		
		US Operations Philosophy	20	1	5		
		The Basics of the Taiwan Situation	20	1	5		
		Code Algorithms	36/20	2	7		
		Military Intelligence	36	2	3		
		Military Planning	54/36	3	4		
Fundamental Specialty Courses	Electives	Computer Fundamentals	36/20	2	1		
		Science and Technology Document Retrieval	20/12	1	2		
		Multimedia Technology	36/20	2	4		
		Signals and Systems	54	3	4		
		Complex Functions	54	3	3		
		Numeric Analysis	72	4	6		
		Fundamental Circuit Theory and Experiments	54/36	3	3		
		Analog and Digital Circuits and Experiments	90/40	3	4		
		Total Number of Credits for Elective Fundamental Specialty Courses (at least 15 elective credits for each student)				35	

Course Classification		Information Security		Periods/Lab Hours		Credits		Semester Schedule	
		University Information	Military Information						
		Security Branch Academy	Security Specialty						
		Required	Electives	(A)	(B)	(A)	(B)	(A)	(B)
		Courses (A)	(B)						
		Network		36/20		2		4	
		Security							
		Protocols							
		Network		36/12		2		4	
		Security System							
		Structures							
		Security		36/12		2		5	
		Evaluation							
		Standards for							
		Information							
		Technology							
		Scanning for		36/20		2		5	
		Hidden							
		Troubles in							
		Networks							
		Security		36/20		2		5	
		Certification							
		Technology and							
		Application							
		Computer Virus		54/36		3		5	
		Program Design							
		and Application							
		Preventing and		36/20		2		6	
		Remedying							
		Computer							
		Viruses		36/20		2		6	
		A Study of							
		Hacker Attack							
		Methods							
		Network		54/36		3		6	
		Intrusion							
		Detection and							
		Defending							
		Against Attack							
		Emergency		36/20		2		7	
		Response and							
		Mishap							
		Recovery							

Recovery Technology for Protecting Against Electromagnetic Radiation Leaks	36/20	2	7
Network Management	36/20	2	7
Information Attack and Defense Tactics	36/20	2	7
Total Number of Credits for Required Specialty Courses		26	

Course Classification	Information Security University Information Security Branch Academy Military Information Security Specialty Required Courses (A)	Periods/Lab Hours		Credits		Semester Schedule	
		(A)	(B)	(A)	(B)	(A)	(B)
	Information Warfare and the New Revolution in Military Affairs		20		1		3
	C ⁴ I Confrontation Fundamentals of Mathematic Modeling		20		1		3
	Foreign Military Command Systems		54/30		2		4
	Target- Oriented Program		36		2		4
			54/36		3		5

Specialty Courses	Electives	Application Management Information Systems	36	2	6
		An Introduction to US and Taiwan Social Information Systems	36	2	6
		Software Engineering	54/36	3	7
		Lectures on Systems Security Technology	36	2	8
		Introduction to Systems Security Systems Engineering	36/20	2	7
		Synthetic Experiments for Information Security Technology	54	3	7
		Total Number of Credits for Elective Specialty Courses (at least ten elective credits for each student)			

(4) Teaching Plan for the Fundamental Specialty Courses for Economic Information Security
Information Security

University Information Security Branch Academy	Periods/Lab Hours	Credits	Semester Schedule
---	----------------------	---------	----------------------

Course Classification		Security Branch Academy Military Information Security Specialty	Periods/Lab Hours		Credits		Semester Schedule		
		Required Courses (A)	Electives (B)	(A)	(B)	(A)	(B)	(A)	(B)
		Management		36		2		3	
		Management Information Systems		36		2		4	
		A Survey of Electronic Commerce		36		2		3	
		Security Technology for Operating Platforms		54/36		3		4	
		Security Technology for Databases		54/36		3		4	
		Oracle Language		72/54		4		6	
		C Language Program Design		54/40		3		3	
		Data Structures and Algorithms		54/30		3		2	
Fundamental Specialty Courses	Required Courses	Information Theory		36		2		5	
		Network Principles and Communication		72/40		5		6	
		Database Fundamentals and Application		54/30		3		3	
		Coding Principles		72/40		4		3	
		Operating Systems		54/36		3		4	
		An Introduction to Codes		72		4		6	
		Introduction to Information Security		20		1		3	

and Regulations 20 1 3

Total Number of Required Fundamental Specialty Credits 45

Course Classification	Information Security University Information Security Branch Academy Military Information Security Specialty		Periods/Lab Hours		Credits		Semester Schedule		
	Required Courses (A)	Electives (B)	(A)	(B)	(A)	(B)	(A)	(B)	
Fundamental Specialty Courses	Electives	Macroscopic Economics		36		2		2	
		Microscopic Economics		36		2		2	
		Marketing		20		1		2	
		Accounting		36		2		3	
		Financial Management		20		1		3	
		Computer Fundamentals			36/20		2		1
		Science and Technology Document Retrieval			20/12		2		2
		Compiler Language			72/54		4		4
		Applied Planning and Management			54/36		3		4
		Multimedia Technology Complex			36/20		2		5

Functions			
Basic Circuit			
Theory and	54/36	3	3
Experiments			
Analog and			
Digital	90/40	5	4
Circuits and			
Experiments			
Total Number of Elective Fundamental			
Specialty Credits (at least 12 elective		32	
credits for each student)			

16 April 2003, Chengdu Command [\[501\]](#)

At Chengdu Command, one of Shen's previous military units, he focuses on IW instead of information security. He gave a briefing on how "hot" IW has become particularly in the cognitive area. Shen notes that the center of gravity in the Iraq war revolved around the psychological war as much as it did around the US' comprehensive military operations. IW attacks on the psyche, he states, target the cognitive system. He states that a person without energy, a soul, or thought processes is nothing more than a corpse. This indicates to Shen that the cost-effectiveness of IW is far higher than that of armed warfare. Shen's focus on the media's involvement in PSYOP indicates to him that the scope of war has become broader. Like other authors, Shen also writes that the Iraq war was a performance for a global audience, a display of IW's comprehensive and intangible aspects.

Shen states that one must understand the impact of IW attacks on the psyche from the perspective of strategy. While information is objective, people's powers of observation, judgment, and decision making are subjective. The objective conditions of war in Iraq must be viewed from the ideological perspective of IW according to Shen. He further notes

The objective of IW is to achieve control. The key to achieving effective control is in controlling the psyche but this is extremely difficult. War today is no longer a tool to be operated independently by politicians, as people outside of the political realm have more means and capabilities of suppressing war.

Shen believes that US Secretary of Defense Donald Rumsfeld was correct in stating that advanced weapons and the information threat were as important as the use of ground forces. He notes that IW is the center of gravity for the RMA and summarizes the rise of IW in two points. First, the function of information is continually increasing, and it has become a third major

First, the function of information is continually increasing, and it has become a third major strategic resource after material and energy (with the media at the front line). Second, the destructiveness of war is based on precise information weapons far in excess of what people can imagine. But he believes Rumsfeld was not thoroughly informed on Sun Tzu's theory of war and therefore neglected the fact that IW is a People's War in the true sense of the term and includes different means of combat. He also states combining China's Art of War and China's thinking about guerrilla warfare together with modern technology reveals infinite power. US efforts relied too much on advanced technology and overlooked the use of stratagems and tactics. Modern war requires fusion among the old and the new, the soft and the hard, and brains and brawn.

Shen believes that IW's technological-equipment developments need to occur in tandem with improvements in tactics and thinking with a focus on the guiding role of theory. This stands in sharp contrast to US thinking, he believes, whose primary focus is on technology. The imagination is the source of IW tactics and IW has brought about changes in global strategic trends. A fertile imagination is a key to developing a trump card weapon, which is thinking about something that others cannot. China is not far behind the US in IW equipment and it is definitely ahead in the area of theory according to Shen.

June 2003 Interview in Warrior News[\[502\]](#)

The article in Warrior News used in Deciphering Information Security was a question and response period between Shen Weiguang and officers and troops of the Guangzhou Command. During the interview process he continually emphasized the importance of personnel, both their physical capability to endure long deployments and their mental capabilities to handle the requirements of the information age. As Shen notes

Even though modern war is moving in the direction of high technology and over-the-horizon radar, the decisive factor determining victory on today's battlefield is still personnel, especially individual combat personnel. Enhancing the degree to which common soldiers are able to control technology requires large investments in terms of time and money, which is why the educational requirements for soldiers are going up, and is one of the main reasons that most countries place high demands on educational backgrounds when selecting soldiers.

Shen answered a question regarding the PLA's current communications equipment and how it could function in future wars. He states that when confronting electronic interference, one must make use of instantaneous message transmissions or the use of intermittent message transmission. If there is interference over the entire frequency range one must engage in command and control via radio platforms using modulation or an unfix frequency band. The best method to confront interference, he notes, is to update equipment and enhance its technological content.

Another question was directed at the character of war. Shen answered that the conventional patterns of war have been discarded in favor of new terms such as information control, integrated air-ground operations, joint operations, and soft countermeasures. Psychological warfare, propaganda warfare, economic warfare, trade warfare, grain warfare, and personnel warfare continue to appear on the scene. For military operations, a nonlinear, extensive model characterized by psychological penetration, air strikes, long-range strikes, and joint ground operations is currently the most appropriate model. It is designed to control the enemy's

enemy.

China must put an extensive effort, Shen noted, into incorporating networks among firepower platforms, operational units, and their combat systems. Information operations can only be enhanced by the horizontal and vertical coordination of these combat systems. At the same time Shen warns about the psychological effects or espionage potential of all of this integration. For example, he states that a cell phone might be a signal source that produces electronic interference in the brain and that a keyboard in front of the computer may be a platform for making someone (via control of their thoughts) to divulge secrets. Shen concludes that one needs to be cognizant how modern information technology has turned signals and text into weapons.

28 May 2002, Armed Police Forces[503]

Shen's lecture to the People's Armed Police was dedicated to antiterror operations under new conditions. While this was the first lecture he presented chronologically it was left until last due to its antiterror theme.

Shen began by explaining several characteristics of the information age as he normally does when lecturing. IW's strategic goal, he states, is to destroy the enemy's will to start and engage in a war. At the level of combat, it is to disrupt the enemy's decision making processes. At the level of tactics it is to paralyze the enemy's system of force. Now nonviolent types of war are directed against leaders. War can be unseen, and it need not involve bloodshed. The trend toward nonviolent and soft war is characterized by the following features.

- First, the goals of war have changed from territorial expansion and economic aggression to information plundering and targeting psychological elements. A concept such as network warfare is designed to attack the opponent's central nervous system, which is his C4I system.
- Second, the function of information has undergone a transformation from a subservient status to the status of a guide.
- Third the patterns of war are evolving from the tangible to the intangible.
- Fourth, victory is sought by nonviolence.
- Fifth, the goal of war is zero deaths.
- Sixth, war is developing in the direction of miniaturization.
- Seventh, one should learn how to make use of the media since information can either strengthen or break up national cohesiveness and national power.
- Finally, computer programmers can fight wars from either their offices or homes. Remote manipulation of warfare is now a given and IW might be considered fighting war from indoors.

Given this background, Shen then proceeds to tell the audience that the new century has witnessed the introduction of terrorism as the new form of war. To prevent terrorism in China, Shen recommends that the country continue to rely on prevention, prevention, prevention. This includes gaining an understanding of the characteristics of terrorist activities and gaining a grasp of the operational rhythms of the war against terror. This includes focusing on areas where terrorists choose to act and where no one takes notice such as areas under no one's jurisdiction or areas

by groups devoted to dividing the nation, organized crime, and individual criminal elements. To fight these elements will require increased coordination among the various combat forces and the proper division of responsibilities between the military and the police Shen notes. New types of tactics must be developed. Tactics, he adds, refers to a complete collection of elements such as operational thinking, stratagems and methods, and operational initiatives which can be manipulated. That is, a good tactic must be able to be converted into a combat plan and be flexible. Police training must be expanded and include special operations as a key component and not as an optional element.

解密信息安全
Deciphering Information Security
Shen Weiguang
July 2003

Table of Contents

Chief Author: Shen Weiguang
Publisher: Xinhua Publishing House
Date of Publication: 2003

Introduction: Courageously Climbing the Summit of Military Theory...1
Foreword: Ten Tasks Facing China's Information Security Field...1

Information Security Research

1. Studying a Framework for a National Information Security Support System...3
2. Strengthening China's Information and Network Security Building...26
3. China's Present Information Security Situation and Tasks...68
4. Extremely Urgent Training for Information Security Personnel...119

University Programs for Information Security

1. Foreword...127
2. Strategic Orientation...127
3. Program Architecture...132
4. Moving Plans Forward...190
5. Risk Management...192
6. Conclusions...193
7. Attachments...194

Information Warfare Research

1. Ideal War and New Trends in War...241
2. Information Warfare Research and Theory Innovation...259
3. Development Trends in World War—Reducing Destructive Force...285
4. The Media Field Is Becoming the Forward Position in Information Warfare...320
5. "Hot" Cold Thoughts on Information Warfare—Talking about the Use of Information Warfare in the Iraq War...336
6. Operations and Training under Informationized Conditions—Linking Answers from Situations in the Iraq War with Questions from Some Officers and Enlisted Personnel

6. Operations and Training under Informationized Conditions—Linking Answers from Situations in the Iraq War with Questions from Some Officers and Enlisted Personnel in Guangzhou Military Region...	360
7. Antiterrorist Operations under the New Circumstances...	380
8. A Proposal that the People's Armed Police Establish an Information Warfare Center...	406
Postscript...	519

CHAPTER SEVEN: AN INTERPRETATION OF NETWORK CENTRIC WARFARE

This chapter summarizes key chapters of editor Wong Zieh Deh's An Interpretation of Network Centric Warfare, 2004.[504]

Introduction

PLA academicians and policy makers closely study current US military developments. Perhaps no issue has come under closer scrutiny than the concept of Network Centric Warfare (NCW). The PLA has followed the doctrinal development and practical application of this concept in the various US branches of service and also in the policy and vision statements that the Defense Department issues periodically.

The PLA's stated purpose for publishing An Interpretation of Network Centric Warfare is to study foreign military methods, absorb their experiences, and master the rules of military-informationization building in order to help the transformation of the Chinese military from a mechanized to an informationized force.[505] Chinese military leaders believe that NCW is one of a handful of key concepts that China must master if it is to be truly competitive on today's battlefield. Further, the work demonstrates to the US reader how thoroughly the Chinese understand US NCW theory and practice (the book is better than most US explanations of NCW). An Interpretation of Network Centric Warfare underscores for the US reader that the Chinese truly believe in the stratagem of "know the enemy and know yourself and you will win every battle." On a much smaller scale the book covers how the PLA is implementing a Chinese-based NCW concept.

The Forward to An Interpretation of Network Centric Warfare notes, "this book systematically analyzes the underlying framework, development strategy, and component elements of network centric warfare and offers enlightenment for enhancing the informationization building of China's military." [506] Chief Editor Wong Zieh Deh and his associates (referred to hereafter as "the authors") appear to have accomplished this goal. Chapter headings include the following topics: a description of NCW, the meaning and model of NCW, the C4ISR system of NCW, the global information grid, information superiority and NCW, support technologies for NCW, military mapping and NCW, weapon components of NCW, information security and NCW, operational support for NCW, and battlefield management of NCW. Only the last chapter in the book addresses China's NCW equivalent concept but does so in not nearly the detail as the first eleven chapters. The book's Forward states that "the last chapter of this book specifically suggests a response to network centric warfare and ways to realize leapfrog-style development." [507] Unfortunately, the book actually doesn't go this far. Perhaps there is a classified version of the book not available to the public that does.

The book was researched and written by the PLA's Information Engineering University.

Central Military Commission member and PLA Chief of Staff General Liang Guanglie wrote the Preface. Only a few of the book's twelve chapters will be examined in detail due to the book's length and the familiarity of most US military readers with the US NCW concept (the main aspect of the book). For example, Chapter One, "A Summary of Network Centric Warfare," is just that, an extensive look into the documents that both developed the theory of NCW and how the US put it into practice. The chapter discusses US battle labs, theoretical concepts and documents (Joint Vision 2020 and the NCW concepts of the US Navy, Army, Air Force, Ballistic Missile Defense, and the Marines), the fundamental principles and basic structure of NCW, the functional domains (physical, information, and cognitive) of NCW, and the key areas, prerequisites, and appraisals of NCW among other issues. The chapter concludes with the problems confronting NCW.

Four chapters were chosen for further examination. They are

- Chapter Three—The C4ISR System of Network Centric Warfare
- Chapter Eight—Integrated Weapons in Network Centric Warfare
- Chapter Eleven—Battlefield Management in Network Centric Warfare
- Chapter Twelve—Welcoming New Challenges, the Leaps and Bounds Achievable by Further Development (Chinese views of their NCW equivalent)

The reader is reminded that Chapters Three, Eight, and Eleven are interpretations of how the Chinese visualize the component parts and integration of the US NCW concept. Whether this is a correct interpretation or not is not discussed. What is important is that these are the issues on which the PLA focused attention, what they think is important in our theory.

The C4ISR System of Network Centric Warfare

In this chapter, the authors described the importance of C4ISR to future war, its impact on the mobility of combat forces, and its structural layout and interoperability potential. It is clear that the PLA is very impressed with US advancements in this area, and they are keen to learn everything they can about the functioning of US C4ISR.

Future warfare, the authors note, will be carried out on a six dimensional battlefield composed of ground, sea, air, space, information, and knowledge. Future war will utilize to the maximum extent possible the C4ISR information system due to its fusing and force multiplier effects. The Chinese feel that the C4ISR system is NCW's foundation for network operations and its basic command system. The authors give the US credit for developing not only the C4ISR system but also for adding kill (K) capabilities to the system. This has transformed C4ISR into a C4KISR system since there are now capabilities for target discovery, precise identification, and tracking and killing.^[508] However, it is unclear who actually developed the C4KISR concept. The Chinese discussed this concept in an October 2005 article in *Xiandai Fangyu Jishu (Modern Defense Technology)* without mentioning that this is a US system.^[509] The C4KISR concept also does not appear in any US text.

The authors of *An Interpretation of Network Centric Warfare* write that C4ISR characteristics include its ability to transmit basic battlefield situations in a timely, comprehensive manner; to assist in selecting optimal operational plans; to automatically transmit orders and rapidly report situations to higher authorities; and to produce a highly mobile and tactical C4ISR

system. Further the C4ISR system improves the operational capabilities of the military since it has the ability to collect, process, and transmit information that is used for command, control, and logistical purposes and to assist firepower, mobility, and defensive capabilities. The system also allows strategists at the highest levels to directly monitor and, in some cases, directly control tactical actions.[\[510\]](#)

The C4ISR system increases the mobility of combat actions as it increases the speed at which a force or weapon system operates according to the authors. A C4ISR system also increases command efficiency since commanders can plan strategies at great distances from combat actions and can unify their command orders for all operational actions. Simultaneously, preparation time is decreased due to the collection, processing, and transmission capabilities of the system. Once battle commences, C4ISR allows one to understand which places are most critical on the battlefield and what resources are available to mobilize and assist friendly forces to destroy enemy forces or systems in key areas.[\[511\]](#) As a result, for the next ten years or so, the security of C4ISR systems will be a focus of attention as forces improve their ISR capabilities and move toward multiservice connections, communications, and interoperability. Stovepipe systems will fall into disuse as integrated, networked, and diversified capabilities replace them. Real-time sensor to shooter responses will be achieved.[\[512\]](#)

This chapter devotes the end of its discussion on C4ISR to the architecture and composition of the C4ISR system. It notes that “the entity that is created by connecting a number of objects together is called a system, and the arrangement and ordering of all the component parts within the entity is called the structure.”[\[513\]](#) The integration of systems constitutes the architecture. For the C4ISR system architecture, the authors list three layers. The first layer is the C4ISR overall structure. It includes four layers, strategy-level (national), strategy/campaign level (theater), campaign level (group army or military), and tactical level (division or brigade). There are also service systems (army, navy, air force, and missile forces) in the overall structure. The second layer is the service C4ISR system structure. It has the same four layers as the overall structure but also specialized military systems and some key individual subsystem elements. The third layer is the structure of the functional elements of the C4ISR system. These elements are the processing, monitoring, transmission, security, and secrecy elements. Large scale operational platforms (strategic missiles and aircraft carriers, for example) have C4ISR systems as their functional elements.[\[514\]](#)

The concept of interoperability requires that systems have a framework when being developed. Frameworks are studied from the perspective of operations (tasks and activities and information exchanges required), systems (associated system capabilities and characteristics with operational requirements), and technology (a minimal set of rules governing the arrangement, interaction, and interrelationships of some of the system components).[\[515\]](#)

With regards to the composition of the C4ISR system, it is composed of command and control systems, an intelligence subsystem, a communication subsystem, and a surveillance and monitoring subsystem. Only the integral components of each will be listed here:

- Command and control hardware and software subsystems: information processing, transmission, and monitoring hardware systems; and battlefield (terrain mapping,

analysis, and environmental processing software), combat analysis (situational maps), simulations (exercises), evaluation (combat loss and efficacy), staff operations, monitoring and detection, mobilization, firepower support, and air defense software systems

- Intelligence subsystems: optical detection system (visible light, infrared, and TV), radar detection, radio reconnaissance, ground sensors, and data fusion systems
- Communications subsystems: internal communications (telephones, intercoms, broadcasts, multicasts, and audio recordings) and external communications (command post links to information sources, operational forces, neighboring units, and upper and lower command centers).
- Surveillance and monitoring subsystems: space-based monitoring system, an aviation monitoring system, a ground-based monitoring system, and a sea-monitoring system. [\[516\]](#)

Integrated Weapons in Network Centric Warfare

Informationized weapons are those that use computers, networks, microelectronics, information, data fusion, and other technologies in unison. Informationized weapons include, but are not limited to, munitions, operational platforms, special reconnaissance equipment, detection and jamming equipment, digitized individual soldier equipment, and automatic command systems. The Chinese break informationized weapons into categories that include special-use information weapons for IO (such as strategic or tactical C4ISR systems), electronic warfare aircraft and early warning aircraft, electronic jamming equipment or electronic jamming bombs, reconnaissance and early warning satellites, computer virus weapons and network logic bombs, new information weapons (such as various missiles, munitions, bombs, and land mines), and traditional weapons that have been “informationized” (filled with information technologies).

The authors of [An Interpretation of Network Centric Warfare](#) state that NCW weapons are of four types: inner space, outer space, information space, and psychological space. Inner space weaponry includes the weapons of the army, navy, and air force. Army weapons in NCW include ground battlefield monitoring systems, mobile ground weapons, and air attack weapons. Navy weapons include surface combat weapons such as the Nimitz Class nuclear powered aircraft carriers and Burke Class destroyers. Underwater combat weapons include Seawolf Class submarines and Los Angeles Class nuclear-powered attack submarines. Air Force weapons include tactical aircraft such as the F-117 Stealth Bomber and the F-16 Fighter. Strategic bombers include the B-2A Stealth Bomber and the B-52 Stratofortress. Early warning aircraft include the E-3 Sentry Early Warning Aircraft and the E-8 Battlefield Surveillance Aircraft.

Outer space weaponry includes those weapons that engage in combat more than 100 kilometers from the surface of the earth. The objective of outer space weaponry is to take and maintain space supremacy with military space forces as the main combat force. Weaponry in this category includes space reconnaissance and monitoring weaponry such as satellites. China considers twenty-first century space weapons to include laser weapons, particle beam weapons, microwave weapons, and antisatellite weapons.

Information space weapons include computer virus weapons, network attack weapons (solid-state virus attack weapons, computer virus guns, chipping attack weapons, silicon-eating

bacteria, and nanometric robots), and electronic countermeasure weapons (radar countermeasure equipment, communications countermeasure equipment, photoelectric countermeasure equipment, and hydro-acoustic countermeasure equipment).

Finally there are psychological space weapons. The authors consider the status of psychological warfare to be more prominent than ever before, stating that it has become the highest form of combat in information operations as well as an important component of a force's combat strength. In this sense, the book is in agreement with Dai Qingmin's appraisal of the rising importance of PSYOP in the information age in Chapter Five. Psychological warfare is defined as the purposeful and intentional transmission of specific information to the enemy's military and civilian populations via operational methods such as psychological propaganda, psychological deterrence, psychological interference, and psychological deception. The three distinguishing traits of psychological warfare are that, first, it is combat against the will of the people and it has an ideological element. Second, the main weapons are the media and information. Spoken and written language, music and song, graphs and pictures, and audio and video recordings are the main information methods used in psychological warfare. Third, psychological warfare does not differentiate between peacetime and wartime.[\[517\]](#)

Strategic psychological warfare is psychological operational actions carried out at a country's diplomatic or national defense level to influence the overall war decisions of foreign leaders and foreign command organizations before and during war. Campaign psychological warfare is carried out in important stages of war and tactical psychological warfare refers to psychological operational actions carried out on the level of operations of ordinary scale.[\[518\]](#)

There is both offensive and defensive PSYOP. The fundamental concept of offensive psychological operations includes psychological propaganda, deterrence, harassment, and deception. Propaganda now includes network and mobile phone propaganda. Such propaganda is voluminous, timely, specific, true, and vivid. Deterrence uses the principles of restraint and intimidation for its power. Harassment includes electronic howling devices and weapons that attack the mind with images. The Chinese accuse the US of using high-powered sound transmission or Hypersonic Sound Systems (HSS) that disturb the enemy's judgment or cause clear-headed soldiers to become confused. Finally, deception includes several different types of strategies where the goal is to win and defeat the enemy via stratagems. Defensive psychological weapons and measures include patriotism, the ability to adequately prepare for psychological defensive operations, the necessity to carry out the required management of wartime news and public opinion, the necessity to occupy the frontlines of propaganda in the fight for public opinion, and the unleashing of psychological counterattacks against the enemy's psychological attacks.[\[519\]](#)

Battlefield Management in Network Centric Warfare

Battlefield management in network centric warfare is defined as relevant measures taken to carry out the unified organization, planning, control, and utilization of the information environment, information facilities, frequency spectrum resources, societal elements, and personnel in the theater of operations. NCW enables real-time discovery and destruction, and it alters the traditional operations cycle of observe-orient-decide-act. NCW characteristics are "small, extensive, far, direct, fast."[\[520\]](#) This will cause Chinese forces to overhaul or reform the way they think in terms of command and management according to the authors of *An Interpretation of*

Network Centric Warfare.

Even though watching the wars in Afghanistan and Iraq from afar, the PLA nonetheless listed several principles facing battlefield management. First NCW makes the ground battlefield three-dimensional in the sense of being tactical (direct and kinetic energy weapons), operational (intelligent robots), and strategic (nuclear, biological, and chemical). Second, the sea battlefield is multidimensional in the sense of utilizing the ground, sea, air, space, and electromagnetic spectrums. This includes mobile airfields and launch platforms, over-the-horizon vessel formations, dirigibles, shore-based aircraft and missile boats, and cruise missiles. Third, the air battlefield is becoming even more violent. This is due to the precision and the added power of modern munitions. Fourth, the electromagnetic battlefield densely covers the ground, sea, air, and space fronts. Finally, the first battle is now more decisive due to NCW. The science and technology of NCW now determines techniques, tactics, and strategies.[\[521\]](#)

The forms, measures, and methods of NCW operations are fundamentally different from traditional operations. The battlefield is more expansive and includes the function of managing the battlefield due to the increased demands caused by weapons management, managing computer network systems and military and civilian information systems, and managing frequency spectrum resources.[\[522\]](#) Management must be systematic. NCW also requires strict regulations and a legal basis for battlefield management.[\[523\]](#) The central goal of battlefield management in NCW is to improve NCW's operational capabilities and to lower personnel casualties and the loss of equipment. Such improvement ensures that operational forces carry out their combat missions safely, orderly, quickly, and with cover.

A basic task of battlefield management is to create a systems' effect that is organized and coordinated.[\[524\]](#) One such system is the system of frequencies. Effective methods and measures must be taken to assign, monitor, and manage the frequency spectrum resources on any battlefield. A separate organization must be created to organize frequency resources since they are a special type of weapon. People forming this organization should come from the communications department of all units. They should plan, allocate, monitor, and manage the use of the frequency spectrum in a theater of operations or on the informationized battlefield. This requires knowing both enemy and friendly capabilities and making judgments on strong and weak points in these capabilities. Even in peacetime, repeated testing of strategic-level, campaign-level, and tactical-level operational networks in special operations labs must be conducted.[\[525\]](#) This will enable the development of a systematic principle with a function of increased efficiency in which $1 + 1$ is greater than 2.[\[526\]](#)

The Chinese view NCW as placing increased emphasis on psychological battlefield management. This is because of two factors. First, highly precise and intelligent weapons make war more brutal, intense, and complex than ever, placing an additional psychological load on combatants. There is also an increased soft destruction of the psyche caused by the use of special media that utilizes speeches, texts, images, sounds, and emails to carry out this type of mental combat. This requires militaries to psychologically mold their officers and enlisted personnel, to teach the development of control over one's emotions and judgments, to pay attention to the methods and measures by which the enemy launches psychological warfare, and to control public opinion and negative psychological influences.[\[527\]](#)

Meeting Challenges and Achieving Leapfrog-style Development

This chapter discusses in more detail how the Chinese might apply NCW. First, the PLA considers NCW to be a new form of warfare. NCW has changed how strategies, campaigns, and tactics are applied and requires adjustments in the functions, authorities, missions, and focus of commanders at all levels.[\[528\]](#) Second NCW links together situational awareness, command and control, software attacks, and other capabilities.[\[529\]](#) It is likely that Chinese theorists are discussing how NCW is changing traditional military thinking. Such talk must also be objective and realistic in the establishment of superiority and trump cards.

NCW involves ingraining “jointness” in the minds of participants. Dividing lines among systems must be shattered and strength created through joint technology, tactics, regulations, and organization. This ensures that the entire combat effectiveness of the system will be brought into play.[\[530\]](#)

A challenge for PLA network administrators is to properly set up information fusion technology for subscribers as the web becomes more complex. Just as Metcalf’s law states that there is a direct ratio between a network’s power and the square of the number of nodes on the net, so too an increase in the number of nodes increases the degree of complexity of the network. This raises stricter demands on the operation and management of the system. There appears to be a direct relation between the cube of the number of nodes on a system and the system’s complexity according to the authors.

Informationized warfare has also influenced operational objectives, a weapon technology’s composition, and an armed forces organizational structure. The foundation for informationized war is composed of two issues, integrated comprehensive information system and informationized weapons. Backward systems of organization usually reject advanced military theories. In the information age new systems of organization must be developed to capture these advanced information theories. There remains the need for an authoritative department to carry out centralized and unified management and coordination and for a mechanism to develop strategy and support.[\[531\]](#)

The RMA has set off a worldwide adjustment to military strategy in many countries, and this has pushed the transformation of organizational systems to center stage. Future work entails developing an operational theory for informationized warfare that can counter the US military’s NCW concept. Future work also includes the development of the functions and missions of China’s military. Technology determines tactics and tactics determines organization. It is hoped that the armed forces integration concept will result in a multifunctional force with information weapons and with operational units grouped together based on their different missions.[\[532\]](#) The national defense science and technology management system must also be transformed, with top-down design programmed to yield analysis, research, and demonstrations. Top-down design should continue in conjunction with the Central Military Commission’s strategies and policies for the new period that include preparations for military struggles such as high-technology based limited wars. The Chinese believe authoritative management is needed, and thus it is recommended to establish a leading organization for military-wide informationization building.[\[533\]](#)

The PLA is moving ahead with the production of informationized equipment. They continue to improve system countermeasure capabilities, to promote the transition from electronic warfare toward NCW, and to achieve leapfrog-style development in the information operations building of the armed forces. The PLA notes in this chapter, for example, that China has already joined the ranks of leading world producers of high-performance computer industry technology and parallel processing technology. China has made great advances in its own research and development of Linux source code-based operating system software and all kinds of trade application system software. It has domestically produced databases, information security software, and application software for electronic government, electronic commerce, and industry informationization. A situation that was completely dominated by foreign countries and that threatened China's information security software industry is being ameliorated bit by bit. Thus China sounds confident in its information-age developments and ability to catch up with the West.[\[534\]](#)

This focus on civilian industry is not by accident. Military authors note that, without a doubt, information technology personnel are a resource that will have to be relied upon when high-technology warfare unfolds. The personnel system of the armed forces will have to enlist computer hackers or treat them as wartime reserves and give them preferred treatment to provide technical support for military building and operations.[\[535\]](#) Information system building must focus on integrated information support capabilities, information countermeasure capabilities (focused on informationized firepower attack capabilities), and comprehensive full-spectrum protection capabilities (focused on information system protection). A comprehensive battlefield information system should become the basis for achieving the transformation for operations centered on platforms to operations centered on informationized warfare. Confrontation between systems will occur in future wars. This means that China must have a systems' strategy that is long-term, radial, and collapsible backed up by a unified standard using common software. Communication networks, computers, database management systems, interfaces with weapon systems, data, and secure services must be integrated. Further the global information grid must support the "three nets in one"—the sensor net, the weapons platform net, and the information net—in informationized warfare theory.[\[536\]](#) There is also a need to research and explore the development of future strategies in IW and joint operations capabilities.[\[537\]](#) The PLA is researching trump card developmental strategies as well as trump card capabilities for strategic and campaign IW measures. The PLA hopes to create, among other things, IW deterrence and real-war capabilities.[\[538\]](#)

Conclusions of this author with regard to An Interpretation of Network Centric Warfare are contained in Chapter Ten, Conclusions.

An Interpretation of Network Centric Warfare

Wong Zien Deh, Chief Editor

2004

Table of Contents

Chief Editor: Wong Zien Deh

Publisher: National Defense Industry Press, Beijing, China

Date of Publication: May 2004.

1. A Summary of Network Centric Warfare
 - 1.1 The Origin of Network Centric Warfare
 - 1.1.1 How Network Centric Warfare Came into Being
 - 1.1.2 The Model of Network Centric Warfare
 - 1.1.3 A Distant View That Is Becoming Clearer
 - 1.2 The Concepts and Composition of Network Centric Warfare
 - 1.2.1 Operational Concepts Related to Network Centric Warfare
 - 1.2.2 Fundamental Principles of Network Centric Warfare
 - 1.2.3 The Basic Structure of Network Centric Warfare
 - 1.2.4 The Functional Domains of Network Centric Warfare: The Physical Domain, the Information Domain, and the Cognitive Domain
 - 1.2.5 The Strategic Commanding Elevation in Network Centric Warfare
 - 1.3 The Key Areas of Network Centric Warfare and Their Technology Goals
 - 1.3.1 The Key Areas of Network Centric Warfare
 - 1.3.2 Technology Goals of the Key Areas
 - 1.4 Prerequisites for Network Centric Warfare
 - 1.4.1 Creating an Environment for Innovation
 - 1.4.2 Accelerating Transformation in Military Affairs
 - 1.5 Network Centric Warfare Appraisal Analysis
 - 1.5.1 The Fundamental Substance of Network Centric Warfare Appraisal Analysis
 - 1.5.2 A Model for the Degree of Maturity of Network Centric Warfare
 - 1.5.3 Operational Tests of Network Centric Warfare
 - 1.5.4 Conclusions of the US Military's Study of Network Centric Warfare
 - 1.6 The Difficult Problems That Network Centric Warfare Is Facing
 - 1.6.1 Theoretical Problems That Network Centric Warfare Is Facing
 - 1.6.2 Technical Problems That Network Centric Warfare Is Facing

2. Network Centric Warfare: Its Meaning and a Model
 - 2.1 The Substance of Network Centric Warfare
 - 2.1.1 The Aims of Network Centric Warfare
 - 2.1.2 The Essence of Network Centric Warfare
 - 2.2 Fundamental Model of Network Centric Warfare
 - 2.2.1 The Fundamental Model of Network Centric Warfare of the US Army
 - 2.2.2 The Fundamental Model of Network Centric Warfare of the US Navy
 - 2.2.3 The Fundamental Model of Network Centric Warfare of the US Air Force
 - 2.3 Fundamental Characteristics of Network Centric Warfare
 - 2.3.1 Real-Time Sharing of Battlefield Information, Accelerating the Operations Tempo
 - 2.3.2 The Flattening of the Chain of Command; Command Efficacy Is Notably Enhanced
 - 2.3.3 All-Service Joint Operations; the Degree of War Integration Is Improved
 - 2.3.4 Operational Actions Are Highly Coordinated; Warfare Is Conducted in All Directions
 - 2.3.5 Battlefield Transparency Is Increased; Victory or Defeat in War Depends on Information Supremacy
 - 2.4 The US Military's Strategy for Realizing Network Centric Warfare
 - 2.4.1 Study Real War Problems; Come Up with a Development Strategy for Network Centric

Warfare

2.4.2 Attach Importance to Top-Down Design; Accelerate the Building of the Information Infrastructure

2.4.3 Reform the Military System; Adapt to New Forms of Operations

2.4.4 Advancing System Tests and Developing Network Centric Warfare Theory

2.4.5 Building a New Force and Enhancing the Build Up of the Informationized Battlefield

2.5 The Concepts and Role of Network Centric Warfare

2.5.1 Network Centric Warfare Is a Necessity for the Development of Warfare in the Information Age

2.5.2 The Philosophy Manifested by Network Centric Warfare

2.5.3 The Role of Network Centric Warfare in Future Wars

2.5.4 The State of Development of US Network Centric Warfare Capabilities

2.5.5 The US Military Is Determined to Fight Network Centric Warfare

3. The C4ISR System of Network Centric Warfare

3.1 The Evolution of the C4ISR System of Network Centric Warfare

3.1.1 From C2 to the C4ISR System

3.1.2 The Main Characteristics and Functions of the C4ISR System

3.1.3 The Status and Role of the C4ISR System in Future Warfare

3.1.4 The Impact of the C4ISR System on Future Operations

3.1.5 The State of Development of the C4ISR System

3.2 C4ISR System Architecture

3.2.1 A Model of C4ISR System Architecture

3.2.2 The Architectural Framework for a C4ISR System

3.3 Basic Composition of the C4ISR System

3.3.1 The Command and Control Subsystem

3.3.2 The Intelligence Subsystem

3.3.3 The Communications Subsystem

3.3.4 The Reconnaissance and Monitoring Subsystem

4. The Global Information Grid

4.1 The Connotation of the Global Information Grid

4.1.1 The Definition of the Global Information Grid

4.1.2 The Global Information Grid Is the Application of Information Grid Technology in the Military Arena

4.1.3 A Reference Model for a GIG Network Environment

4.2 The Architecture of the Global Information Grid

4.2.1 Implications of GIG Architecture

4.2.2 The Overall Framework of the GIG

4.2.3 Operations System Architecture of the Global Information Grid

4.3 The Role and Status of the Global Information Grid

4.3.1 The Global Information Grid Is an Important Channel for Pursuing Information Superiority and Decision Making Superiority

4.3.2 The Global Information Grid Is the Cornerstone of Network Centric Warfare

4.4 The State of the Buildup of the US Military's Global Information Grid System

- 4.4.1 The Basic State of the Grid Being Built by the Navy and the Marine Corps
- 4.4.2 The Basic State of the Grid Being Built by the Air Force
- 4.4.3 The Basic State of the Grid Being Built by the Army
- 4.5 Development Trends of the US Military's Global Information Grid
 - 4.5.1 Complete Fusion with the C4ISR System
 - 4.5.2 Developing New Functions
 - 4.5.3 Achieving Information Security Assurance

- 5. Information Superiority in Network Centric Warfare
 - 5.1 Capturing Information in Network Centric Warfare
 - 5.1.1 Ground-Based Reconnaissance in Network Centric Warfare
 - 5.1.2 Air-Based Reconnaissance in Network Centric Warfare
 - 5.1.3 Sea-Based Reconnaissance in Network Centric Warfare
 - 5.1.4 Space-Based Reconnaissance in Network Centric Warfare
 - 5.1.5 Network Reconnaissance in Network Centric Warfare
 - 5.2 Information Fusion in Network Centric Warfare
 - 5.2.1 Cognitive Information Processing
 - 5.2.2 Data Fusion Technology
 - 5.2.3 The Joint Service Imagery Processing System (JSIPS)
 - 5.2.4 The All Source Analysis System (ASAS)
 - 5.3 Information Distribution in Network Centric Warfare
 - 5.3.1 Individual Soldier Information Systems
 - 5.3.2 The Joint Tactical Information Distribution System (JTIDS)

- 6. Support Technologies for Network Centric Warfare
 - 6.1 Network Technology under Network Centric Warfare Conditions
 - 6.1.1 Technology for Linking Networks
 - 6.1.2 Network Transmission Technology
 - 6.2 Gateway Technology under Network Centric Warfare Conditions
 - 6.2.1 Gateway Functions
 - 6.2.2 Difficulties with Gateways
 - 6.2.3 Hierarchical Structure of Gateways
 - 6.3 Sensor Network Technology in Network Centric Warfare
 - 6.3.1 Sensor Network Architecture
 - 6.3.2 The Use of Unmanned Aerial Vehicles and Unmanned Vehicles
 - 6.3.3 Sensor Networking
 - 6.4 Early Warning Technology in Network Centric Warfare
 - 6.4.1 Space Early Warning Technology
 - 6.4.2 Airborne Early Warning Technology
 - 6.4.3 Computer Network Early Warning Technology
 - 6.5 Information Transmission Technology in Network Centric Warfare
 - 6.5.1 Broadband Communications Technology
 - 6.5.2 High Fidelity Information Security Transmission Technologies
 - 6.5.3 Compatible and Interoperable Technology
 - 6.6 Tactical Data Link Technology in Network Centric Warfare
 - 6.6.1 A Summary of Tactical Data Links

- 6.6.2 The Present State of Development of Tactical Data Links
- 6.6.3 Development Trends in Tactical Data Links
- 6.7 Identification Friend or Foe Technology in Network Centric Warfare
 - 6.7.1 Network Defense Technology
 - 6.7.2 Cipher Technology
 - 6.7.3 Integrated Identification Friend or Foe System Technology
- 6.8 Network Confrontation Technology in Network Centric Warfare
 - 6.8.1 Spears in Network Confrontation: Network Attacks
 - 6.8.2 Shields in Network Confrontation: Network Defense

- 7. Military Mapping in Network Centric Warfare
 - 7.1 The Digital Battlefield and Military Mapping
 - 7.1.1 The Digital Battlefield
 - 7.1.2 The Digital Spatial framework
 - 7.1.3 Remote Sensing Technologies and the Space-Based Comprehensive Information Network
 - 7.1.4 Military Geographical Information Systems
 - 7.1.5 Military Mapping Support
 - 7.2 The Role of the US Military's National Imagery and Mapping Agency in Network Centric Warfare
 - 7.2.1 Goal and Mission of the US Military's National Imagery and Mapping Agency
 - 7.2.2 The US Military's National Imagery and Mapping Agency's Concept of Network Centric Warfare
 - 7.2.3 The US Military's National Imagery and Mapping Agency's Ideas on Network Centric Warfare Operations
 - 7.2.4 Contributions of the US Military's US Imagery and Geospatial Information System to the Global Information Grid
 - 7.3 Network Centric Warfare and the Global Satellite Positioning System
 - 7.3.1 The Concept of the Global Positioning System and Its Support Base
 - 7.3.2 The Most Recent Developments in the Global Positioning System Technology of the US Military
 - 7.4 Network Centric Warfare and Space-Based Network Information Fusion Technology
 - 7.4.1 Space-Based Network Information Fusion Technology
 - 7.4.2 Space-Based Information Networks' Support of Network Centric Warfare
 - 7.4.3 The Substance of Information Fusion Processing in Network Centric Warfare
 - 7.4.4 The Function of Space-Based Information Fusion Technologies in NCW

- 8. Integrated Weapons in Network Centric Warfare
 - 8.1 Inner Space Weapons
 - 8.1.1 Informationized Weapons Munitions
 - 8.1.2 Army Weapons
 - 8.1.3 Navy Weapons
 - 8.1.4 Air Force Weapons
 - 8.2 Outer Space Weapons
 - 8.2.1 Space Reconnaissance and Monitoring

- 8.2.2 Twenty-first Century Space Weapons
- 8.3 Information Space Weapons
 - 8.3.1 Computer Virus Weapons
 - 8.3.2 Network Attack Weapons
 - 8.3.3 Electronic Countermeasure Weapons
- 8.4 Psychological Space Weapons
 - 8.4.1 Psychological Offense Weapons and Methods
 - 8.4.2 Psychological Defense Weapons and Methods
- 9. Information Security in Network Centric Warfare
 - 9.1 The Main Security Threats Confronting Network Centric Warfare
 - 9.1.1 The Threat of Potential Danger to Systems
 - 9.1.2 Threats to the Physical Environment
 - 9.1.3 The Threat of Information Attacks
 - 9.1.4 Threats from Inside Personnel
 - 9.1.5 Threats from Poor Management
 - 9.2 Key Information Security Technologies in Network Centric Warfare
 - 9.2.1 Information Security Technologies in Identification-Friend-or-Foe Systems
 - 9.2.2 Security Control Technologies in Weapons Control Systems
 - 9.2.3 Security Safeguard Technology in Information Transmission Systems
 - 9.2.4 Security Technology for Networking Various Network Platforms
 - 9.2.5 Network Defense Technology in the Network Centric Warfare System
 - 9.2.6 Electromagnetic Information Protection and Network Survivability Technology
 - 9.3 Information Security Support Systems for Network Centric Warfare
 - 9.3.1 Building a Secure Network Platform
 - 9.3.2 Building Information Security Infrastructure
 - 9.3.3 Building a Support System for Organization Management
 - 9.3.4 Formulating a Strategy for the Development of Information Security
- 10. Operational Support in Network Centric Warfare
 - 10.1 Command Support in Network Centric Warfare
 - 10.1.1 Command Support Requirements in Network Centric Warfare
 - 10.1.3 The Thinking Behind Building Command Support for Network Centric Warfare
 - 10.2 Battlefield Building Support in Network Centric Warfare
 - 10.2.1 Requirements for Battlefield Building Support in Network Centric Warfare
 - 10.2.2 The Keys for Building Up the Battlefield in Network Centric Warfare
 - 10.2.3 The Thinking Behind Battlefield Building in Network Centric Warfare
 - 10.3 Organizational Structure Support for Network Centric Warfare
 - 10.3.1 The Requirements for Organizational Structure Support for Network Centric Warfare
 - 10.3.2 The Key Points of Organizational Structure Support in Network Centric Warfare
 - 10.3.3 The Thinking Behind Building the Organizational Structure for Network Centric Warfare
 - 10.4 Logistics Supply Support for Network Centric Warfare
 - 10.4.1 The Requirements of Logistics Supply Support for Network Centric Warfare
 - 10.4.2 The Key Points of Logistics Supply Support in Network Centric Warfare

- 10.4.3 The Thinking Behind Building Logistics Supply for Network Centric Warfare
- 10.5 Military Personnel Support for Network Centric Warfare
 - 10.5.1 The Requirements for Military Personnel Support for Network Centric Warfare
 - 10.5.2 The Quality Makeup of Military Personnel for Network Centric Warfare

- 11. Battlefield Management in Network Centric Warfare
 - 11.1 The State of Battlefield Management in Network Centric Warfare
 - 11.1.1 Fundamental Characteristics of Force Organization and Operational Actions
 - 11.1.2 The Circumstances Facing Battlefield Management for Network Centric Warfare
 - 11.2 The Characteristics of Battlefield Management in Network Centric Warfare
 - 11.2.1 Expansion of the Range of Battlefield Management
 - 11.2.2 Making the Substance of Battlefield Management Specific
 - 11.2.3 Making Management Measures Intelligent and Management Objectives Systematic
 - 11.3 Implementing Battlefield Management in Network Centric Warfare
 - 11.3.1 Basic Requirements for Battlefield Management in Network Centric Warfare
 - 11.3.3 Implementation of Battlefield Management in Network Centric Warfare
 - 11.4 The US Military's Operational Management of Network Centric Warfare
 - 11.4.1 Battlefield Networking, Quick and Easy Management, Weapons with Increased Effectiveness
 - 11.4.2 On the Digital Battlefield, Control Is Strong, and Operations Are More Powerful
 - 11.4.3 "Network Logistics," Precision and High Efficiency, Powerful Support

- 12. Meeting Challenges and Achieving Leapfrog-Style Development
 - 12.1 Challenges to China's Armed Forces Posed by the New Forms of Warfare
 - 12.1.1 Conceptual Challenges
 - 12.1.2 Technological Challenges
 - 12.1.3 The Challenge of Organization
 - 12.2 New Thinking for Achieving Leapfrog-Style Development
 - 12.2.1 Innovating Military Theory
 - 12.2.2 Building a New Combat Command System
 - 12.2.3 Transforming the National Defense Science and Technology Management System
 - 12.2.4 Enhancing the Training of Military Informationization Personnel
 - 12.2.5 Technical Equipment for Developing Informationization

CHAPTER EIGHT: STUDY GUIDE FOR IO THEORY

Chapter Eight is a selection of translated questions and answers to key concepts and terms from a Study Guide for Information Operations Theory, 2005.[\[539\]](#)

Introduction

One of the primary purposes for writing Decoding the Virtual Dragon is to help Westerners better understand Chinese terms and concepts that are information-age related. If one wants to “decode” the Chinese virtual dragon, then one must see how the Chinese define terms. One of the primary Chinese sources that helps enable this goal is the November 2005 Study Guide for Information Operations Theory. Xu Genchu edited the book and the Chief Examiner/Director was Dai Qingmin, a PLA general with whom the reader is now quite familiar. Xu and Dai’s work offers an interesting glimpse into Chinese home-grown concepts and definitions. There are also discussions and descriptions of US and a few other national concepts. The entire volume is published in a question and answer format. In all, there are 400 questions in the text. The Academy of Military Science’s Press printed 10,000 copies of the work.

The text is divided into the several sections listed below (numbers in parenthesis do not represent page numbers for that section but rather the number of the question and its answer listed in the book. For example, “information” contains questions and answers for question 1 through question 20.).

Forward

Part One: Information and Informationization

- Information (1-20)
- Informationization (21-38)
- The New Revolution in Military Affairs (39-51)

Part Two: Informationized Operations

- Information Warfare, Informationized Operations, and Informationized War (52-88)
- Producing and Developing Informationized Operations (89-93)
- The Characteristics, Rules, and Principles of Informationized War (94-106)

Part Three: Information Technology (107-137)

Part Four: Informationized Forces

- Informationized Armed Forces (138-154)
- Informationization of the Armed Forces (155-170)

Part Five: Informationized Weaponry

- Informationization of Weaponry (171-182)
- Informationized Weapons (183-199)
- New Concept Weapons (200-220)

Part Six: Informationized Battlefield Environment

- The Informationized Battlefield (221-239)
- Battlefield Information Systems (240-267)

Part Seven: Informationized Operations Command (268-292)

Part Eight: Informationized Operational Support

- Informationized Operational Logistics and equipment Support (293-305)
- Operational Information Security Assurance (306-322)

Part Nine: Forms of Informationized Operations

- Joint Operations (323-349)
- Informationized Operations of the Military Branches (350-359)

Part Ten: The Military Informationization Buildup and Development in Some Countries

- The State of Development of the US Military's Informationization (360-377)
- The State of Development of the Russian Military's Informationization (378-384)
- The State of Development of the Japanese Military's Informationization (385-391)
- The State of Development of the Indian Military's Informationization (392-400)

Short summaries and descriptions of key concepts are provided below. There are full translations for a few select definitions as well. The book's Table of Contents is listed at the end of the chapter. It provides the reader with the entire list of all four hundred questions. This provides the reader with the full picture of the scope of the book.

In some places the Chinese concept as described matches well with a similar US concept, such as information operations or information warfare. In other cases (informatized war, informationization of the armed forces, etc.) it does not. Types of operations new to the US that are discussed include integrated network-electronic warfare and navigational warfare. In addition, the PLA's focus on a few issues (countermeasures, control, comprehensive) will be stated in **bold** to highlight their use. These terms are not used in IW discussions in the West nearly as much as they are in China. They are terms to be studied for their meaning as potential application measures against non-Chinese forces. Identifying these concepts is an important part of the decoding exercise. As an example, comprehensive was used over 50 times, countermeasure nearly 70 times, and nearly the same number for control (and that number did not include "control" when used in

the sense of command and control) excluding the in the definitions below.

Forward

In the Forward to the book Dai Qingmin states that he is the director of the text and a member of the Advisory Committee for the Informatization of the Military (as of August 2005). He notes that the informatization of military affairs is accelerating both the fundamental transformations in the patterns of war and the **comprehensive** transformation of the military. The strategic objective of the PLA, according to Dai and the Central Military Commission, is to “build up the information-based armed forces and win information-based wars.”[\[540\]](#) This objective includes **comprehensively** enhancing operations more suited to information warfare requirements. Dai feels that knowledge and information are overtaking materials and energy in importance and this will breed new operational patterns of warfare.

Dai notes that information systems are the focus of attention and now include the global information grid (GIG) and C⁴KISR systems. The K factor in the latter is described as the “kill” factor (Dai later defines the factor as being of US origin). These systems “exhibit a high degree of fusion between real-time information transmission, intelligent information processing and scientifically assisted decision making, allowing integrated information support capabilities to become the foundation and support for a new model of operational competencies.”[\[541\]](#)

Multifaceted and **comprehensive** defense capabilities have become the core of operational capabilities and a decisive means of strategic attack in Dai’s opinion. Information **countermeasure** capabilities have become the most significant independent element of these operational capabilities. Dai calls for five types of informatized[\[542\]](#) operational capabilities (the “Five Competencies”), namely integrated information support; fully dimensional early warning reconnaissance; informatized firepower attacks; multifaceted **comprehensive** defending; and multi-level information **countermeasures**.[\[543\]](#)

Dai believes it is necessary to incorporate informatization at every level but also notes that China’s informatization foundation is comparatively weak. Three issues are holding China back: ideology is insufficiently unified, knowledge is not profound enough, and research is not penetrating enough. The PLA has commissioned the Information Operations Theoretical Research Office of the Operations Theory and Doctrine Research Department at the Department of Military Sciences to research the basic issues of informatized operations and help overcome these shortcomings. This volume, Study Guide for Information Operations Theory, is a result of this research effort. It is Dai’s hope that the guide “will have a definite value as a guide and reference for unifying ideology and awareness, spreading foundational knowledge and deepening theoretical research to become a friend and scholar to officers, soldiers and theoretical workers.”[\[544\]](#)

Informationization

24. What Is Informatized Military Thought?[\[545\]](#)

Dai states that military thought reflects the general characteristics and patterns of military matters. Informatized military thinking is the combination of informatized thinking and military thinking expressed as informatized military activities. The key to informatized military thought is in

achieving information superiority, and the goal is to protect the information frontier and information sovereignty, to solidify information defense at the national level, and to win future wars. The core of informatized military thought is information guidance, which is grasping the essential characteristics of information and understanding the form in which the value of information is expressed. One must gain **control** over the impact that information and information activities have upon war.

33. How Do We Establish a Theory of Informatization with Chinese Military Characteristics? [\[546\]](#)

Dai states that there are three requirements for building an informatized force. The first requirement is for applied research to set out strategic guidance. He lists a number of research topics (which again highlight the Chinese focus on strategy) for study, to include the strategic environments of military informatization around the world; the overall strategy for the building of informatization forces; the development and utilization of the military's information resources; strategies for the buildup of the military's information networks; strategies for incorporating information technology into weapons and equipment; the structural organization of informatized armed forces; strategies for military informatization security; and strategies for training personnel.

Another requirement for the informatized buildup of the military is developing the guiding theory for information operations. This primarily involves establishing a basic framework for a theoretical system of information operations, to include research into the militaries of advanced nations around the world, especially the US military. A final requirement is fused theoretical research. This primarily includes the fusion of informatized operations theory with the theory of People's War; the fusion of informatized operations theory with active defense strategy; the fusion of informatized operations theory with deterrence strategy theory; the fusion of military informatization buildup with the theory of strong science and technology in the military; and the fusion of military informatization buildup theory with spatial military power buildup theory.

The New Revolution in Military Affairs

39. What Is the Relationship between the Informatization of the Armed Forces and the New Revolution in Military Affairs? [\[547\]](#)

Dai writes that the new revolution in military affairs is the process of changing the mechanized military into an informatized military. Instituting the informatization buildup of the armed forces is what the new revolution in military affairs fundamentally entails. Building up informatized armed forces and winning information wars are the basic goals of the new revolution in military affairs and are the goals of the buildup of the informatized armed forces.

41. What Is the Essence of the New Revolution in Military Affairs? [\[548\]](#)

Dai notes that the essence of the new revolution in military affairs lies in the transformation of the pattern of mechanized military affairs from the industrial era into the pattern of informatized military affairs in the information era. The pattern of military affairs is a general term referring to all manifestations of military affairs during a specific period of historical development. It includes military theory, warfare practices, military organization, weapons and equipment, military personnel, logistical safeguards, systems of military service, and war mobilization.

44. What Are the Main Characteristics of the New Revolution in Military Affairs?[549]

The first characteristic is making contact with every aspect of the patterns of military affairs, and every realm they touch upon, so that they are fundamentally transformed. This includes objective factors such as the budget for national defense, military technology, weapons and equipment, the leadership and command structure for the armed forces, the organization of the forces, military training, the caliber of military personnel, logistical safeguards, reserve forces, the system of military service and the structure of war mobilization. The subjective factors include military theory, military thought, military ideas, and ways of thinking about the military, etc. A second characteristic is that this reform is occurring in many countries, particularly the major nations of the world. (Author's note: Dai's explanation of objective and subjective factors in this section fits well with Peng and Yao's description of these topics in Chapter One of Decoding the Virtual Dragon.)

45. What Are the Possible Developmental Trends of the New Revolution in Military Affairs?[550]

Dai writes that prior to the year 2020, the new revolution in military affairs may occur primarily in the military technology and equipment sectors. This includes microelectronic technology, computer technology, communications technology, sensor technology, and information technology groups related to software engineering technology. Newly-developed weapons and equipment containing a high degree of information technology are intelligent weapons systems. The various reconnaissance and warning systems, C4ISR systems, precision-guided munitions, and information warfare weapons are produced one after another, pushing simple mechanized military technology and equipment from its historical stage.

From the beginning of 2020 to early 2040, the development and creation of military thought and theory may become the mainstream of the new revolution in military affairs. In one respect, military theory will be guided by the revolution in technology and equipment. In another respect, military theory will learn from information and technology outside military affairs. It will utilize this information to guide the entire reform. Military concepts will experience a revolutionary change and military theory will become innovative. From early 2040 to the middle of this century, the revolution in the structural organization of the military may become the mainstream for the new revolution in military affairs.

47. What Are the Main Effects of the New Revolution in Military Affairs on War?[551]

The impact of the new revolution in military affairs on war is primarily as follows:

- First, the causes for wars are becoming more complex. While economic interests may remain as the basic impetus for war, the increase in interaction between nations and between various political forces may lead to more conflict between nations, peoples, and social groups in terms of political, diplomatic, and psychological factors. This has led to an upswing in religious and ethnic conflict. These types of conflicts act as a type of predisposition for future wars.
- Second, war objectives are even more limited now. In the information era, where war is becoming more "transparent" to the majority of people, leaders will need to place severe restrictions on the progress and goals of war.
- Third, there are now many new types of warfare. War in the information era involves not only countering the armed forces of other nations and weakening the enemy's industrial

base, but also involves destroying its information systems. Multiple types of new operations will appear, such as information warfare, precision warfare, **controlled warfare**, paralysis warfare, invisible warfare, and computer virus warfare.

- Fourth, death and destruction in war have been reduced, comparatively speaking. The object will be to avoid indiscriminate bombing that causes an enormous loss of life and to avoid desperate and decisive battles between large groups of soldiers.
- Fifth, the duration of war will be shortened. The rhythm of war will be quickened, and operational actions will occur in real-time to a degree. This means that real-time detection and the discovery of targets will result in real-time command, real-time mobilization, real-time strikes, real-time evaluations of destruction, and real-time support. Tasks which in previous wars took several hours or even longer to complete now take only a few minutes or even just a few seconds. Wars will be much shorter owing to restricted war objectives and the smaller scale of warfare.
- Sixth, there will be a greater degree of transparency on the battlefield. In future wars, the side with information superiority will have its information network systems working nonstop to transfer real-time intelligence to its computers. Combat personnel who are dispersed over the battlefield will receive these images at the same time, enabling them to better understand the conflict.
- Seventh, the fight to achieve information supremacy will be especially fierce. A superior brigade becomes “deaf, dumb, and blind” the minute it loses **control** over information. A weaker force that gains superiority in the area of information can also **control** the initiative on the battlefield.
- Eighth, the degree to which warfare is integrated will be unprecedented. Distinctions between levels of strategy, campaigns, and tactics will become blurred. The various types of operational systems such as combat forces, combat support forces, and combat logistical support forces will connect with the various operational functions such as battlefield intelligence, command, **control**, communications, and strikes to form an organic whole.
- Ninth, command over operations will be very difficult and demanding. There are four areas for consideration. Command is performed in real-time, or near real-time—if not, opportunities are lost and a person becomes passive. Command is always performed in the midst of action. Command requires a frequent need for vertical-lateral communications. And coordination is complex, especially laterally-coordinated missions.
- Tenth, there are new aspects as to how force is concentrated. For example, quantity is being replaced by the concentration upon capability and quality. The large scale use of precision-guided weapons and stealth weapons means that battles or strategic objectives can be realized with just one or two artillery strikes. Integrated, joint operations will become the basic form of operations.

48. What Are the Main Effects of the New Revolution in Military Affairs on Operation Theories? [\[552\]](#)

Dai notes that as reforms push forward, modern operations theory is entering a period of profound change. First, there are new theories of force. While traditional operations forces revolve around troops and tangible objects (destructive force and mobility of tanks, ships, planes,

artillery, and munitions), information exerts an enormous impact on combat, serving as a critical amplifier of combat power and strength. Computational capabilities, communication capacities and reliability, real-time reconnaissance capabilities, and computer simulation capabilities are becoming key elements in weighing military power. Military force is premised today on an intangible and enormous potential which is difficult to quantify. It comes from the structural power of information weapons systems.

Second, the vertical, stratified relationship between strategy, combat, and tactics is changing. Information weapons systems have formed new space-time relationships where space has expanded and time has shrunk. This, in turn, has caused a fundamental change in the vertical and stratified relationship between strategy, combat, and tactics. Information weapons systems can exceed time and space in terms of communication and command. They also possess near real-time long-range precision strikes, which means that tactical strikes can achieve their strategic objectives immediately.

Third, **we are moving beyond traditional concepts of attacking and defending**. Future wars will witness greatly enhanced capabilities in the areas of vertical depth reconnaissance, long-range communication, precision strikes, and long-range attacks. Operational actions will be conducted simultaneously at every layer, in every direction, and in every aspect of the entire operations space. The stable front and the fixed battlefield no longer exist. The line between attacks and defensive actions is also no longer so clear owing to the high degree of flow and uncertainty on the battlefield. As such, the view of operations theory guiding defense and the comparatively stable battle lines for attacks is being replaced by an entirely new theory of thinking. (Author's note: One Chinese military author, Dong Zifeng, who Dai did not cite, writes that **control** is the operational concept whose importance is now equal to that of attack and defend.)

Fourth, the basic operational principles of the past are being broken down. On the information-based battlefield of the future, for example, the goal of annihilating the enemy's effective strength will be replaced by attacks upon the center of gravity and information nodes of the enemy's operational system. There will be more focus on the principle of concentrated force.

49. What Are the Main Effects of the New Revolution in Military Affairs on Forms of Operations? [\[553\]](#)

The new revolution in military affairs, Dai states, will further accelerate the changes to forms of operations. First, **controlling** the information is a precursor to contending for dominance on the battlefield. **Controlling** the information refers to fully grasping the power to acquire, **control**, and use battlefield information, while not allowing the opponent to exercise these powers. Information is the anchor for decision making and strategy in war. **Controlling** battlefield information means dominating battlefield information and providing the initiative in war. **Control** enables a weaker opponent to defeat a stronger one.

Second, the basic form of attack has become a full-depth precision strike. "Full-depth" refers to an attack on the primary targets in the entire operational space. Full-depth precision strikes will become the basic form of firepower attacks on future battlefields.

Third, direct combat is no longer the primary form of combat. Instead of engaging in direct contact with the opponent, various types of long-range indirect firepower weapons and munitions placed at long distances are used to destroy and defeat the opponent in place of tanks and other types of direct-aim weapons. This is why future combat will not be conducted at close range.

Fourth, **countermeasures** will involve entire systems. In future wars, **countermeasures** between sides will involve all services, multiple departments, and multiple types of weapons and equipment. These **comprehensive countermeasures** will depend upon large systems which will include advanced information, monitoring and reconnaissance systems, advanced command and control systems, and precision-guided munitions. There are two aspects to these overall systems: First, the information systems, nonfatal technology systems, and precision strike systems will form an integrated weapons and equipment system that is integrated into the entire structure of the armed forces to form an even better **comprehensive countermeasures** capability. Second, enemies need to be visualized as a system made up of connected elements. The system, or the centers of gravity of the system (nodes), needs to be targeted for attack such that the entire combat system is paralyzed and broken down.

51. How Do We Understand the Revolution in Military Affairs with Chinese Characteristics?[554]

For an understanding of a revolution in military affairs with Chinese characteristics, one needs to take a scientific approach to the five basic issues guiding the revolution: the target tasks, the core, the model, the path, and the developmental steps.

(1) Target tasks. The goal of the Chinese military has changed from winning local wars under general conditions to winning regional wars under conditions of modern technology, especially high technology. China needs to build up their informatized armed force since that is the starting point for theory and practice for the revolution in military affairs with Chinese characteristics.

(2) The core of the revolution. It is vital that the informatization of the armed forces be at the core of the revolution in military affairs. The Central Military Commission totally supports this contention, indicating that there has been a critical change to the benchmarks and primary technical paths for building up the Chinese military. The transformation of the structural organization of the armed forces must be beneficial to the fast and ordered flow of information, along with utilizing information flow to **control** the flow of materials and energy to develop weapons and equipment.

(3) Building a model. The demands placed upon the armed forces model by informatized warfare require excellent soldiers, decisive information victories, and high quality science and technology to determine the military's combat power (represented by information technology). The goal of the intensification of science and technology, along with quality and efficiency, is to grasp the results of the transformation of the conditions of modern warfare and to possess the sharp features of the revolution in military affairs.

(4) The basic path. As China attempts to institute the leapfrog development of its military transformation, stress must be placed on informatization without discarding mechanization, as the latter is an objective requirement of informatized warfare. The acceleration of the integration of mechanization with informatization must continue.

(5) Developmental steps. The “Three-Step Development Strategy” and the “Two Major Strategies”^[555] stipulate the goals and steps for the revolution in military affairs with Chinese characteristics. China will have continuity and stability in its policies if it can adapt to the developmental trends and strategies of the world revolution in military affairs and combine them with the actual conditions of the Chinese nation and the Chinese military. Today not advancing means retreating, and this requires that China finds a consensus in the area of theory so that patterns of informatized operations can be found.

Information Warfare, Informatized Operations, and Informatized War

52. What Is Information Warfare?^[556]

The prominent status of information as an important strategic resource and a guiding factor in deciding wars has allowed the concept of information warfare to develop. The primary operational mean in information warfare is information energy while operational targets are the enemy’s information, information systems, and systems of knowledge and belief. The fundamental goal remains to gain information superiority.

A scientific definition of information warfare requires an objective analysis of the structural elements of war and these are materials, energy and information. They help form the objective world, and they are the basic structural elements of war. In the information era, however, information is the lead element. IW increases not only the destructiveness and mobility of materials (primarily weapons), but adds more important and completely new capabilities such as intelligence and structural power. Intelligence refers to materials with intelligent (human) capabilities, such as unmanned vehicles, robots, smart bombs, and intelligent C4ISR systems. Structural power refers to individual operational units that are decentralized on the battlefield (including personnel and weapons) and connected by information into an enormous organic whole that forms a formidable and monolithic resultant force. This implies that information now **controls** materials and energy dependent on whether the free flow of information is obstructed or not. Information flow includes the acquisition, transmission, processing, and utilization of information. IW’s actions must permeate into every node in the information flow.

Historically, information warfare first appeared as an item in Military Terms Used by the People’s Liberation Army of China published by the Academy of Military Sciences in September of 1997 according to Dai. It was defined as “**countermeasure** activities in the information realm performed by two sides in a conflict, primarily in contending for information resources, in gaining the initiative in the production, transmission and processing of information, and in destroying the enemy’s information transmission as a means of creating favorable conditions for containing or winning a war.”^[557] Thus this focus on **countermeasures** has been in the Chinese IW definition for ten years now.

Broadly defined, IW is also known as strategic information warfare, and refers to two sides use of **countermeasures** and combat using information and information technology to gain information superiority in politics, the economy, science, technology, diplomacy, culture, and the

military, during peacetime or in times of war. The narrow sense of information warfare is that it is the information **countermeasures** that two sides utilize to gain information superiority. Dai states this is what the US military calls “battlefield information warfare.” It includes intelligence warfare, electronic warfare, network warfare, and psychological warfare. Electronic warfare serves as IW’s foundation. The broad and narrow IW concepts are often intertwined and act upon one another. This was demonstrated during the 1999 war in Kosovo when Yugoslavia and its supporters instigated fierce network attacks against NATO countries that also affected, in Dai’s opinion, military actions on the battlefield.

The Chinese military was among the first to propose the idea of information warfare. The definition currently employed by the Chinese military typically uses the narrow sense of information warfare. The more consistent view holds that information warfare consists of military **countermeasure** actions using information operations and other related operational powers to achieve and maintain information superiority.[\[558\]](#)

While defining IW later in the text (Author’s note: see question 74, Intelligence Warfare) Dai listed numerous methods for the classification of information warfare. In the area of the various types of operations, you have offensive information warfare and defensive information warfare. In the area of information sources, you have public information warfare and secret information warfare. In the area of the layers of operations, you have strategic information warfare, combat information warfare and tactical information warfare. When it comes to geographical area, you have domestic information warfare and international information warfare. In the area of intelligence itself, you have political information warfare, economic information warfare, military information warfare, commercial information warfare and diplomatic information warfare. When it comes to the methods of information acquisition, you have human information warfare and technical information warfare.[\[559\]](#)

53. What Are Information Operations?[\[560\]](#)

The concept of information operations is controversial according to Dai. There is no consensus whether IO encompasses information warfare or whether the opposite is true. Many believe that information operations actually equate to the narrow sense of information warfare while other analysis reveals two separate layers of meaning within the concept of IO. One layer refers to using operational powers that focus on military **countermeasure** actions to gain and maintain information superiority. Here this refers to the information operations phase or the form of information operations. The second layer refers to the utilization of professional operational powers that focus on military **countermeasure** actions that target the information systems of the enemy. So layer one is focused on gaining information superiority and layer two is focused on targeting. The latter includes electronic warfare or network warfare. The layers are different in methods, means, purposes, and organizational planning.

There are three IO definitions. The first is as follows:

“Information operations refer to operations used to gain and maintain **control** over information.” This definition expands IO’s domain since there are quite a few ways to gain and maintain **control** over information. For example, firepower attacks obviously fall under the category of firepower warfare, and they cannot be defined as information operations just because

they are capable of destroying information equipment and systems.

The second definition is:

“Information operations refer to a series of operational actions employed by two sides in a conflict in which the enemy’s information systems are used or destroyed and one’s own information systems are protected as a means of gaining the power to acquire, **control**, and use information.” There are many methods for the use, destruction, and protection of information systems. Many firepower wars, special operations, and techniques and tactical means for protecting information systems are also clearly not covered by information operations.

The third definition is:

“Information operations refer to a series of operational actions undertaken to gain and maintain information superiority on the battlefield or **control** over information. The two sides in a conflict use electronic warfare or computer network warfare to use or destroy the information and information networks of the enemy and protect one’s own information networks as a means of acquiring, **controlling** and using information.” This defines IO in terms of content but not patterns. It is not rigorous or scientific.

Information operations are conducted around information with the aim to gain **control** over information. This requires that information media be **controlled** as well as information’s content and efficiency. Information media refer primarily to signals **controlled** by destroying the transmission and reception of the enemy’s signals while protecting one’s own. **Controlling** the content of information means that one must use information’s content to attack an enemy and to prevent an enemy attack. The efficiency of information refers to information’s function. Information eliminates uncertainty and serves people. **Control** of people’s minds lies at the core of **controlling** the efficiency of information. The two major goals of IO are to destroy the enemy’s information and information systems while protecting one’s own and to destroy the enemy’s cognition and beliefs while protecting one’s own. This implies attack and defense attitudes and fully explains why information operations are not electronic warfare centric (the use of information media such as signals to destroy information transmissions) but also include computer network warfare and psychological warfare (the use of information’s content to destroy information systems along with human cognition and beliefs).

The targets of information operations are information, information systems, and the cognition and beliefs of people. The means employed in information operations include information (both information media and information content) and weapons and equipment dedicated to attack information systems. Information operations involve both attacking and defending. The domain of information operations revolves around information **countermeasures** on the battlefield. In summation, information operations are defined as a series of **countermeasures** employed by two sides in a conflict in which information or weapons and equipment **controlled** by information and dedicated to the destruction of information systems are used in order to influence and destroy the enemy’s information, information systems, and cognition and beliefs, along with preventing the influence and destruction of one’s own information, information systems, and cognition and beliefs in the same manner by an enemy.

54. What Are Informatized Operations?[561]

Dai notes that the concept of informatized operations was an original creation of the Chinese military based upon the changes it experienced in the areas of the patterns of war and the forms of operations. Broader than IO, **it is the same or similar in many respects to the concepts of “integrated operations” and “network-centric warfare” held by militaries abroad.**

Dai states that the Chinese military’s comprehension of informatized operations is not yet consistent. The war in Iraq offered one view, that the signature patterns of warfare have shifted from mechanized war to informatized war. This means that a new model for **countermeasures** on the battlefield has already been formed. Another view is that the patterns of war are still in the beginning stages of the transition from mechanization to informatization and that future informatized war has not completely moved beyond the mechanized warfare model. An analysis from the perspectives of historical and dialectical materialism shows that the latter understanding makes more sense. One can say that informatized operations are the advanced stage of operational patterns in an informatized war. They represent the future direction of military **countermeasures** on the battlefield.

So what exactly are informatized operations, then? They can be defined as follows: two sides in a conflict rely to a high degree upon information, information systems, informatized weapons, and equipment. This involves information flow and systematic **countermeasure** actions undertaken in multiple spaces and realms such as on land, on the sea, in the air, in space, in the electromagnetic realm, in the realm of information, and in the realm of cognition.

The most prominent feature of informatized operations is that they are integrated operations guided by information and seeking information superiority. Their internal mechanism involves the effective **control** of other systems via the use of intelligent decision making systems so that information superiority can be converted into superiority in the areas of space-time, decision making, and action to create and exercise better efficiency. Their outer manifestations are characterized by **comprehensive** precision operations which are the circular, seamless links formed by precision perception detection, precision transmission distribution, precision decision making **control**, precision attack evaluation, and precision support safeguards. The elements thus formed include informatized weapons and equipment, combined operations powers, the full-dimensional digital battlefield, networked information systems, and integrated operations actions according to Dai.

56. What Is Informatized War?[562]

Qian Xuesen, a renowned scientist in China, notes that the war model for the twenty-first century is informatized war under the nuclear deterrent.

Dai writes that the basic way energy is released is in the form of an integration of information with energy whose platform is information network war. Informatized war is a new pattern of war, a high-technology war that exploits the knowledge economy and information era for its energy. Informatized war corresponds to the patterns of the informatized military.

Dai adds that a **comprehensive** understanding of informatized war requires that two faulty

understandings about it are corrected: namely, that informatized war is “politics without bloodshed,” and that victory comes solely by relying upon information. First, war involves fierce military **countermeasure** activities undertaken by two sides in a conflict for specific political and economic purposes. It is the continuation of politics by the use of violent means. Informatized war is one type of war and is still within the categorical domain of war. The fundamental view of Marxism is still valid for understanding future informatized wars. The essential political nature of war, the just and unjust nature of war, and the hierarchy of the scales of war have not changed due to the advent of informatized war. Therefore the view that informatized war is “politics without bloodshed” is wrong. Second, from the perspective of the moving status of war, each new pattern of war supersedes the existing pattern of war. The meaning of “supersede” here does not refer to complete negation. Without the weapons and equipment of mechanized war, information and energy have no material support and no platform from which to operate. The idea that the goals of war can be achieved by relying upon information only is impractical.

Shen Weiguang would disagree with Dai on the first point. He notes that due to information, wars can be won without bloodshed in some instances. Many communist party members of the old Soviet Union would agree with Shen. They feel that NATO defeated the Warsaw Pact through the use of information technology and psychological operations.

57. What Are the Various Concepts for Informatized War?[563]

The concept of informatized war, Dai writes, includes the concepts of time and space, of energy, of systems, of **control**, and of the success or failure of informatized war. For informatized war, the choice of time and space for military action is the reflection of using one’s superior military art skills. Military art skills are reflected when the right military unit is deployed at the right time and into the right space. This often decides whether or not the operational effectiveness of an operational element is fully and successfully exploited.

Informatized war quite naturally takes less time. Long-range precision strikes have expanded the battlefield space. These types of time and space changes have had a direct impact upon creating operational theory, choosing operational methods, and building operational power. Energy use in informatized war is reflected primarily in information capabilities that can achieve operational objectives on their own or by guiding the release of mechanical and chemical capabilities.

In terms of the concept of systems for informatized war, the **countermeasure** features of time and space for systems have brought forth great changes. First, the strategy, combat, and tactics for informatized war are integrated as are the various military services. Second, information networks are the foundation and support for an integrated operational system, unifying various operational spaces into one whole entity. This forms a larger system for informatized operations. Third, the integration of the military with civilian society is tighter and interlinked. The construction of an operational system is based upon civilian support to a certain degree now.

In terms of the concept of the **control** of informatized war, the scale, range, and the degree of attacks in traditional wars often far exceed the ability of the instigator to **control** them which often works against the original intentions of the instigator. Now the scale of war, size of war zones, and the force of attacks can be **controlled** precisely. When it comes to strategy, the commander-in-chief

relies on an information network spread across the globe to gain a clear understanding of the status of an entire war zone and to exert continuous **control** over an entire war. When it comes to combat, commanders in war zones rely upon an information network on the battlefield to exert real-time **control** over operations. When it comes to tactics, operations personnel on the battlefield can use precision **control** over weapons platforms and weapons systems to make precision strikes on targets and reduce collateral damage. Now commanders in informatized war not only **control** their troops and their weapons systems and information networks, but exert **control** over enemy personnel and weapon systems through the use of information deception and obstruction.

In terms of the concept of the success or failure of informatized war, the goal is to **control** the enemy and preserve oneself. The objective of **controlling** the enemy and preserving oneself was exemplified during the war in Kosovo. Here, in 1999, the US military conducted large-scale air raids on Yugoslavia and forced them to surrender under duress without penetrating deep into Yugoslav territory. The success or failure of informatized war is not determined by the ratio of casualties on either side or whether one side has captured the other side's territory, but rather in forcing the enemy to submit to one's will. This again indicates why Dai is so focused on psychological operations.

61. What Is Information Terrorism?[564]

This term refers to the use of information tools such as the Internet to engage in terrorist activities or to provide accommodation for the same. It includes the implementation of premeditated, political attacks on information systems, computer network systems, and computer programs and data, along with the abuse of information systems and the use of information systems to engage in fraud or criminal acts.

Terrorist organizations might use information systems in the following ways:

1. To collect sensitive data on their target
2. To raise funds
3. To keep in contact with members of the organization and transmit secret information
4. To engage in extortion
5. To engage in the spread of propaganda
6. To engage in deception and impose psychological terror upon people
7. To engage in information attacks upon the nation's information infrastructure, such as its financial systems, power grid, and traffic control systems.

62. What Are Information Actions?[565]

Information actions are undertaken in times of peace or in times of crisis or war to attack, destroy, or disrupt an enemy's information and information systems while protecting one's own information and information systems. In this sense, Dai's definition of information actions is the same as the US definition of IO. The concept of information actions is larger than that of information warfare, in that information warfare is only a part of information actions, i.e. information actions undertaken during times of war.

In 2003, a US Defense Report heightened information actions to the level of strategy, explicitly stating that "information actions refer to the strengthening of one's own information

superiority and exerting influence upon foreign perceptions of posture as a means of ensuring that national security strategic objectives are achieved.”

There are five main pillars to information actions. They are information safeguards built into computers, the defense of key information infrastructure, the attainment of information superiority, the management of perceptions, and operational efficiency.

63. What Is Information Space?[566]

Information is intangible and does not exist in a solid dimension. It has no independent operational space, though it can permeate and influence all spaces and play a key role in them. A major change to informatized war in terms of operational space has been the advent of the concept of information space, which includes electromagnetic space, network space, and cognitive space. Electromagnetic space refers to electronic warfare. Network space refers to network warfare. Cognitive space is more complex and refers primarily to psychological warfare, warfare of public opinion, and legal warfare. Focus needs to be placed on operations in intangible space, especially in cognitive space.

64. What Is Strategic Information Warfare?[567]

Strategic information warfare refers to information warfare conducted at the strategic level. Its main features are as follows: it has a broad scope, it involves special forms (psychological warfare, warfare of public opinion, warfare of deception, and media warfare), it involves special targets (especially cognitive ones), it is enormously formidable, and its personnel are specialized. The personnel involved in strategic warfare are not necessarily soldiers but may involve computer experts, international criminal groups, or hackers or terrorist organizations with ulterior motives.

65. What Is Battlefield Information Warfare?[568]

Battlefield information warfare is information warfare occurring within battle or combat space. It refers to the **comprehensive** utilization of the means of information technology and various informatized weapons, operations platforms, and C4ISR systems both in preparation or while conducting battle or combat. It includes **comprehensive countermeasures** in warning, detection and reconnaissance, information transmission and processing, weapons **control** and guidance, operations command and control, camouflage, deception, interference, and **military stratagems**. Since battlefield information warfare interferes with or disrupts the enemy’s decision making process it must be conducted before influencing enemy actions so that the enemy cannot implement coordinated and consistent actions. The steps in this process are winning an advantage in the electromagnetic realm and attaining superiority in the air and on the sea. **Controlling** information means gaining the initiative in combat space according to Dai.

66. What Do the Contents and Forms of Battlefield Information Warfare Entail?[569]

The primary content of battlefield information warfare includes operational confidentiality, military deception, electronic warfare, psychological warfare and firepower destruction. The core objective is to gain the initiative in the acquisition, **control**, and use of information in the combat space. Battlefield information warfare refers to **countermeasures** against information systems that directly impact battlefield success. The primary operational forms for battlefield information warfare are electronic warfare and network warfare. Electronic warfare involves activities such as trickery, interference, damage, and destruction conducted against the enemy’s communications

and radar.

68. What Is the Main Content of an Information Operations Plan?[570]

Dai states that information operations plans are the specific embodiment of the resolve of commanders and the preparations and actions conducted by informatized operations forces. Their content is primarily composed of information operations tasks (the primary means and power to be used); the important aspects of the protection of information systems and information security; the important targets, primary means, and weapons to be used; methods of action for information attacks; a force's tasks; the composition and configuration of tasks for combat; the division of operational stages and the expectations and solutions for each stage; the organization of command and coordination; and the time needed to complete preparations for information attacks or to implement them.

Information attack plans include the status of the information environment, the tasks and major targets of information attacks, the specific initiative and deployment of force for information attacks, and the coordination of information attacks. Information defense plans include the status of the information environment, the primary means and impact of the enemy's information attacks, the major targets and primary means of information defense, the specific initiative for information defense, and the coordination of the information defense system.

In order to draft the best information operations plans, a person needs to implement the resolve of the leaders and use modernized means of command; to start from the most difficult and complex situation in the operational relationship to foresee potential developments; and to do your utmost to shorten the time needed to draft up the plan. In no situation should the implementation of information attacks or defense be delayed due to the drafting of the plan.

69. What Are Information Attacks?[571]

Information attacks refer to the use of **comprehensive** means such as electronic interference, electronic deception, computer virus attacks, network penetration, and psychological attacks that commanders and their command organizations launch under a unified command, with a unified operational objective using dedicated information attack forces or nondedicated forces, to achieve and maintain **control** over information. In addition, information attacks are actions to weaken, destroy, or break down the enemy's entire operational effectiveness to the greatest extent possible. Information attacks are the primary operational means of achieving **control** over information.

Information attack forces include electronic **countermeasure** forces, network attack forces, information entity attack forces, and other information attack forces. Among them, electronic **countermeasure** forces interfere and suppress or deceive and confuse the enemy's information acquisition, transmission, and command and **control** systems. Network attack forces work in computer networks to pilfer, alter, disturb, and destroy information processing and the normal operation of information systems. Information entity attack forces use anti radiation weapons and various types of precision-guided weapons and other firepower to engage in the physical destruction of the enemy's information systems. Other information attack forces, primarily psychological warfare forces, make use of media organizations, intelligence organizations, and propaganda organizations, to cause military deception and psychological disruption in enemy forces.

The major tactics used in information attacks include:

- First, information deterrence. This refers to the concentration and integration of superior troops and weapons to form a military deterrent that shakes the enemy psychologically so that he either dares not act without careful consideration or submits due to fear.
- Second, an information blockade. This refers to the concentration of superior information attack troops implementing large-scale suppressive electronic interference against the enemy's electronic information systems in a given area within a prescribed period.
- Third, information power creation. This refers to the use of electronic camouflage, electronic deception, network deception, and "virtual reality warfare" to conceal what is real and reveal what is false, to confuse, deceive, and arouse the enemy. This causes the enemy's information to be false and judgments and decisions to be mistaken.
- Fourth, information contamination. This refers to the contamination of the enemy's information networks with false information, useless information, and "toxic" information to block the enemy's information channels, or to use information to create "pathologies" or to infect the operating environment for information systems.
- Fifth, information harassment. This is the use of information to attack equipment and systems on the enemy's front line or in rear areas by implementing electronic deception, radio propaganda, and electronic interference to secretly release viruses and engage in guerrilla attacks upon the enemy's information system as a means of inflicting psychological pressure. This is guerrilla warfare within the realm of information actions.
- Sixth, nodal destruction. This refers to troops and weapons information attacks on the enemy's strategic positions (one or more nodes) which have a decisive function for his information and electronic systems. This reduces or destroys the entire operational efficiency of the enemy's electronic system.
- Seventh, system paralysis. This refers to the implementation of a high intensity, hidden surprise attack using electronic interference, a virus attack, electronic weapon or firepower destruction attacks upon an electronic information system or equipment, or certain types of electronic targets integrating soft and hard destruction. This either disrupts system operation or efficiency, or renders it completely inoperable.
- Eighth, entity destruction. This is a planned operation using anti radiation weapons, directed energy weapons, and other conventional weapons of hard destruction behind enemy lines that, in conjunction with information reconnaissance, implements firepower destruction upon electronic information equipment (system) to permanently disable enemy equipment.

70. What Are the Basic Requirements of Operations for Capturing Information Supremacy?[572]

Dai's description of the basic requirements for obtaining information superiority focuses on the attack and the use of strategy. He notes that regardless of whether it is the combat stage during the fight for information supremacy or a fusion of the support actions for information operations in joint (cooperative) actions, the following basic requirements must be followed.

First, attention needs to be focused upon the attack. The special features of the techniques and tactics of information operations emphasize attacking even more than traditional ground, sea, or air warfare. Weaker armed forces must actively master these basic requirements.

The attack is the reflection of the dialectical relationship between annihilating the enemy and preserving oneself, along with aggressive defensive thinking. This is because information defense can only be enacted vigorously when it is integrated with information support actions. It is completely possible that an enemy which is weaker in the area of information will implement an asymmetrical information attack which allows for the special advantages of a People's War.

The requirements for focusing on attacking are that first, substantial intelligence information is required. Second, information attack forces and resources must be focused at the key time and into the key directions. Third, efforts must be focused on launching information attacks before the enemy does to gain the advantages of acting first and achieving information supremacy. Fourth, multiple forms of uninterrupted information attack actions must be adopted in combination to prevent the enemy from catching his breath. Fifth, actions must be coordinated and **comprehensive** and address key points.

Second, the Chinese will focus upon the entire attack. Information operations combine attacking with defending using electronic warfare, computer network warfare, and psychological warfare. With "integrated network-electronic warfare" at their core, information operations also involve means such as keeping operations secret, intelligence warfare, and hard destruction to execute integrated warfare. This is the key to information supremacy. Information systems are human-machine systems with complex structures. A combination of soft means of destruction such as electromagnetic suppression, virus attacks, and network **countermeasures**; hard destruction means such as electronic weapon attacks, Special Forces destruction, and firepower destruction; and mental means of attack such as psychological operations and virtual operations can result in effective operations characterized by a mutual increase in strength and mutual support.

Third, technology and strategy need to be given equal weight. Operations for gaining information supremacy have the significant features of high technology along with a strong strategic component. The objects of these operations not only include the enemy's information technology systems, but also his cognitive systems. Emphasis must be placed upon technological **countermeasures** (to include "trump cards"). Chinese forces need to fully exploit strategy and intimately combine soft, hard, and mental means. In particular, Chinese forces must give full reign to the initiative of the people, their creativity, and flexibility.

71. What Is Information Defense?[573]

Information defense refers to a plan unifying the intentions of commanders and the command organizations to protect the security of one's own information and information systems by engaging in tactics to counter reconnaissance, interference, and computer attacks. They are **comprehensive** means and actions that include attacks and the protection of information systems to ensure information supremacy.

Electronic defense, network defense, systems of military secrecy, and other information

defense forces form the backbone of information defense. The primary tasks are to implement measures against deception, reconnaissance, interference, and destruction within the electromagnetic spectrum; to implement measures against invasion and virus attacks in the realm of computer networks; to prevent the physical destruction of electronic equipment by the enemy; and to engage other information defense forces, such as intelligence organizations and news media to conduct deception against military and intelligence **countermeasures** and psychological **countermeasure** activities.

Information defense requires excellent measures against blockades, destruction, and interference, along with early-warning and information recovery capabilities. Chinese forces need to make **comprehensive** use of information retaliation, proactive interference, psychological attacks, information deception, and physical destruction, along with implementing effective defensive measures integrating the overall with the targeted and the active with the passive. The primary tactics are as follows:

- Concealed defense methods (radiation control and signal concealment)
- Deceptive defense methods (combined use of technical means and tactical measures of information deception such as signal source deception, signal channel deception, and information (content) deception)
- Network defense methods (to include multiple types of electronic information equipment and systems that guard against interference, destruction, and concealment)
- Antistrike defense methods (interference suppression [or virus attacks] against command communication systems and the implementation of information attacks where the concept is offense as defense)
- Information barrier methods (the **comprehensive** use of active and passive electronic interference to conduct interference against the enemy's electronic reconnaissance systems where, again, the concept is offense as defense)
- Management and **control** methods (targeted measures and actions to strengthen the management of personnel involved with secrecy and secret media).

The side with the weaker information operations capabilities must make full use of nondedicated information operations forces to include civilian information systems and personnel. The **comprehensive** use of various types of information defense measures and gaining the initiative are of critical significance in winning at information defense.

72. What Is Information Security?[574]

Information security includes both security for information resources and security for information operating systems. Security for information resources includes guaranteeing the integrity, serviceability, and confidentiality of information and data and controlling access permissions and the methods for data storage and extraction. The security of information operating systems refers to the operation of hardware and software, operating system security, disaster recovery, and prevention of electromagnetic information leaks. The traditional sense of property security no longer applies, as information security is a type of resource and strategic security. National security is no longer composed mainly of territory and resources but rather of intangibles such as information and knowledge. Information has become more important as a resource than materials and energy, Dai notes.

73. What Is Network Psychological Warfare?[575]

Network psychological warfare is a special product of psychological operations during the information era. Computer network technology allows computer networks to act as the medium which makes the difference in the information age. This enables two sides to engage in measures such as psychological propaganda, psychological deception, and psychological deterrence over the Internet in order to break down the resolve of the enemy's military and civilians.

74. What Is Intelligence Warfare?[576]

Intelligence warfare is essentially a struggle for the right to acquire and the right to know information. Two sides in a conflict adopt various means to gather and steal information from one another.

There are both broad and narrow definitions of the term "intelligence." The narrow concept refers to "reconnaissance measures or other methods to acquire knowledge of the various aspects of the situation regarding the enemy's military, politics, and economics, as well as the results of analysis and study of these situations. This is an important basis for military action." Narrowly defined, it refers to intelligence combat undertaken in the realm of the military. Broadly defined, intelligence refers to "the latest intelligence reports." The broad sense of intelligence warfare includes intelligence combat between two sides in a conflict in the areas of politics, economics, military affairs, science and technology, culture, and diplomacy.

75. What is Precision Warfare?[577]

Precision warfare utilizes informatized and intelligent high-precision weapons and equipment to engage in operational actions. Precision warfare (or "precision operations") cannot be understood simply as precision strikes that use precision-guided weapons. "Precision" reflects the **countermeasures** in which two sides engage, as well as the entire process itself. The process includes:

- Accurately observing the battlefield
- Accurately acquiring and processing information
- Precisely determining the location of the enemy's forces, weapons, equipment, and incoming fire
- Implementing command and control precisely and in real-time
- Using operational forces and measures precisely
- Precisely implementing attacks
- Accurately assessing the effectiveness of operations
- Precisely implementing logistical safeguards.

In summation, precision warfare includes precision information, precision **control**, precision movements, and precision strikes. Precision warfare can greatly enhance the combat power of the armed forces, reduce their size, and lower casualties.

The political and strategic nature and limitations of high tech warfare require that military actions and operations stay in step with national policy. The targets, force used, and duration and

style of strike must be chosen to maximize effectiveness and to conform to political requirements and the goals of combat and strategy.

The main features of precision warfare are as follows:

- First, it features a high degree of integration between information and firepower, using information to **control** firepower.
- Second, it is a direct strike to the enemy's center of gravity. The center of gravity is the "center upon which all force and actions rely" for an army, and it is where the armed forces get their freedom of action, combat force, and combat will.
- Third, geographical factors such as distance, altitude, terrain, objects on the ground, the features of the terrain, and international borders have little effect on precision strikes.
- Fourth, its operational area is tiny. Targets are extremely concentrated to within a very limited and narrow space.
- Fifth, its space is expanded. Long-range precision-strike platforms can hit targets from thousands of kilometers away.
- Sixth, material destruction, human casualties, and collateral damage are limited.

76. What Is Electronic Warfare?[578]

Electronic warfare (EW) is also known as electronic **countermeasures**. It is defined as follows: "The general term for the various measures and actions used to weaken or destroy the effectiveness of the enemy's electronic equipment (systems) and to protect the effectiveness of one's own electronic equipment (systems). It consists mainly of electronic **countermeasure** reconnaissance, electronic interference and electronic defense." There are differences in EW and IO. Computer network space differs from electromagnetic space in that the important elements in the computer connect to form an organic and whole space, a new and particular space, in which the computer penetrates throughout the land, sea, air and outer space. It has been called the "sixth space." By contrast, actions in electronic warfare take place primarily in the realm of electromagnetic space. The operational targets for information operations include information acquisition, transmission, and processing systems. EW includes systems using electronic equipment to acquire and transmit information. The IO objective is to obtain information supremacy while for electronic warfare it is to acquire electromagnetic supremacy. Of course, one must first achieve supremacy in the electromagnetic realm in order to gain information supremacy.

EW is one aspect under information operations, and it creates a foundation for the creation of information operations. The advent of information warfare has pushed electronic warfare up to a higher realm.

77. What Is Electronic Reconnaissance?[579]

Electronic reconnaissance includes gathering and analyzing the enemy's electromagnetic radiation signals using electronic **countermeasure** reconnaissance forces. It includes signal intelligence, warnings of threats, direction finding, and position fixing, and it enables attacks and defense. Electronic technology reconnaissance primarily refers to radar reconnaissance, optical reconnaissance, night vision reconnaissance, laser reconnaissance, and television cameras.

Electronic **countermeasure** reconnaissance primarily refers to radar, communication, optoelectronic, and underwater acoustic **countermeasure** reconnaissance.

The tasks for electronic reconnaissance include discovering and determining the tactical technical parameters and position of enemy radiation sources for electronic systems and equipment, ascertaining the patterns of activity and deterrence qualities of electronic targets, and analyzing strong and weak points. This enables one to test the effectiveness of a friendly electronic attack and to organize and implement electronic attacks and electronic defense. Electronic reconnaissance includes direct and advanced reconnaissance, and it must integrate **comprehensive** reconnaissance with targeted reconnaissance.

78. What Are Electronic Attacks?[580]

Electronic attacks are operational actions that utilize electronic attack forces to conduct electronic interference and destruction. The unified command carries out these attacks with the goal of weakening and destroying an enemy's electronic effectiveness. This is an important and aggressive operational means of gaining and maintaining information supremacy. When organizing the implementation of electronic attacks one must concentrate forces and adopt multiple means of destroying the enemy's important electronic equipment.

79. What Is Electronic Defense?[581]

Electronic defenses are the **comprehensive** measures to prevent the enemy from uncovering the electromagnetic signals and operational technical parameters emitted from one's electronic equipment. Electronic defense attempts to eliminate or weaken the harmful impact of electronic interference from the enemy's equipment. This EW aspect entails working against electronic reconnaissance, electronic interference, and attempts to destroy friendly equipment.

Electronic defense's primary tasks are to take multiple measures to prevent the position and electronic radiation of one's own electronic equipment from being discovered, to minimize damage, and to maintain the effective operation of major electronic equipment. When organizing the implementation of electronic defense, one must coordinate entire actions to counter reconnaissance, interference, and destruction; make **comprehensive** use of multiple means of electronic defense such as concealment, deception, prevention, avoidance, and repair; and use offensive actions to ensure the stability of electronic defense.

80. What Is Computer Network Warfare?[582]

Computer network warfare is a series of actions designed to interfere with or destroy the enemy's network information systems while ensuring the normal operation of one's own network information systems. The goal is to gain and maintain network information superiority.

There are broad and narrow definitions for computer network warfare. In the broad sense, computer network warfare is the use of technology and network means of countries, ethnic groups, armed groups, and even terrorists to attain network supremacy and destroy information networks. In the narrow sense, computer network warfare refers to information operation actions where operational command systems weaken or destroy the information and effectiveness of the enemy's computer network systems enabling the attainment of network supremacy.

Computer network warfare is composed of computer network reconnaissance, computer network attacks, and computer network defense. Operations mainly involve the use of armed and equipped network warriors. The means of operations include various types of viruses, logic bombs, and chip weapons developed from computer technology.

Computer network warfare will act as both a deterrent and a means of warfare, and it can have a large and profound impact upon the enemy's politics, economics, and military. It is also an important means of battle for a less well-equipped military against one with formidable strengths in high technology.

81. What Is Command and Control Warfare?[583]

Command and control warfare is the integration and utilization of operational confidentiality, military deception, psychological warfare, electronic warfare, and firepower destruction with the support of intelligence. Proper use of this ability enables one to obstruct the enemy from acquiring information and to influence, weaken, or destroy the enemy's command and control capabilities while ensuring that one's own command and control systems and capabilities are not destroyed by the enemy.

Command and control warfare uses attacking and defending among other methods. Countering command and control refers to not allowing the enemy to acquire information. Reliable intelligence is required to support the implementation of command and control warfare.

82. What Is Structural Destruction Warfare?[584]

Structural destruction warfare (SDF) is a form of operations that destroys the structure of the enemy's force thereby limiting its effectiveness. The effectiveness of structural deception is that it breaks down overall combat strength. Some experts believe that nodal destruction warfare is part of structural destruction warfare. SDF uses direct firepower strikes or special agent sabotage to destroy the physical facilities for the enemy's computer networks. Special agent and Special Forces sabotage might include bombing, high energy laser weapons, electromagnetic pulses, microwave bombs, and biological bacteria to strike key nodes and paralyze the entire network system.

The nodes in a system are connection points between important elements and subsystems within an operational system. The sources for information, materials, and energy within an operational system are the nodes of a system, and the US used this method during the Gulf War. Strategic targets were government organizations, command systems, key production facilities, power and energy systems, production facilities for weapons of mass destruction, the railroad, ports, bridges, airports, and missile positions. The destruction of these nodes "mutilated" the system and eliminated its functioning.

The creation of functional chaos limits an enemy's combat capability. Future battlefield C4ISR systems are such that "pulling one hair affects the whole body": hitting a part affects the whole. Carrying out nodal destruction warfare at the right time might be more effective than other operations.

The Characteristics, Rules, and Principles of Informatized

War

94. What Are the Characteristics of Informatized Operations?[585]

The characteristics of informatized operations include the following items.

First, battlefield spaces are transparent to an unprecedented degree. The various operational platforms are able to share operational information and share information resources. With the battlefield information network, passive and active operational information can be seen clearly allowing for near real-time transmission and processing of information.

Second, with operational effectiveness so high, operations have shortened in duration. Operations carried out under informatized conditions can fuse information networks and combat networks between remote precision strikes and battlefield space, resulting in integrated real-time responses. This allows for an even faster decision cycle.

Third, information superiority has become the key to operations. Both sides in a conflict place extreme importance upon surveillance, using aerospace reconnaissance satellites, airborne reconnaissance planes, ground reconnaissance devices, and intelligence personnel to establish an integrated detection system. Informatized operations are the process of attaining information superiority.

Fourth, the characteristics of integrated operations are prominent. The weapons and equipment used in information warfare with other firepower attack weapons makes for enormously effective attacks that have shown exponential growth. Informatized weapons and equipment are becoming the main type of equipment in war. Informatized operations are integrating joint operations and information and firepower, where reconnaissance and surveillance work in concert together with firepower attacks.

Fifth, information systems have an important position. Both information attacks and information defenses are required. Information superiority requires electronic suppression, network attacks, and hard destruction. Information defenses require setting up defensive structures, using wired communications, engaging in deception and propaganda, and implementing electronic interference.

95. What Are the Patterns of Informatized Operations?[586]

Informatized operations possess both the universal patterns of military operations and unique patterns. Problems are listed below.

First, guiding information. In past operations, battle strength was the integration of energy with materials. By contrast, in informatized wars, information has become the combat force multiplier, in that combat force is equal to the combination of energy and materials multiplied by information. Information has already become the basis and guiding element for the full exploitation of energy and materials. The neutralization of information can cause the neutralization of combat force on today's battlefield.

Second, the survival of the fittest. The survival of the fittest is the general principle for every

war. The weak side can still gain an advantage if its strategic tactics are played right and if it properly utilizes the will of the people, morale, the terrain, and preparations. In the information era, whether a person is subjectively willing or not, one needs to keep up with the developments in the global military revolution, adapt to the requirements of informatized war, accelerate the buildup of the information-based armed forces, and unceasingly improve capabilities for informatized operations.

Third, technical advancement. Informatized operations rely upon network-based military information systems, and by adapting information technology to the utilization of strategic tactics, the force of informatized operations be maximized. Chinese forces need to apply information technology to command and control, intelligence and reconnaissance, communications, weapons, and equipment. They also need to continually innovate tactics and means for informatized operations.

Fourth, system **countermeasures**. Informatized operations amount to **countermeasures** undertaken between one system and another. This prevents any one military service or weapons system from dominating the battlefield. Superiority in perception, intelligence, or decision making is transformed into superiority in operational actions overall—this has become the basic formula for informatized operations.

Fifth, the influence of critical nodes. Several critical nodes in an informatized system have key functions. These nodes are surrounded by unceasing action, development, and changes. Any damage to them greatly reduces their effectiveness immediately or leads to paralysis of the system. These critical nodes are the major points of defense, and they are targets of attack. The initial targets during informatized operations are typically command and control centers and important nodes linking a country's political, economic, military infrastructure, and battlefield information network systems.

Sixth, victory in the realm of aerospace. Whoever has the advantage in aerospace will **control** the air, land, and sea from a commanding height. In informatized military **countermeasures**, communication relies upon satellites as does the transmission of information and battlefield surveillance. Airplane and ship navigation, along with missiles, are guided by using satellites, as is troop positioning. Gaining aerospace supremacy must of necessity become the center of gravity of future informatized operations.

96. What Are the Main Features of Informatized Operations?[587]

The following items explain the main features of informatized operations.

First, operational forces are becoming informatized. Information has replaced materials and energy to become the guiding factor in combat force. The degree to which troops, battlefields, weapons, and equipment have become informatized directly determines how effective combat force and operations are. Armed forces with a high degree of informatization will gain a firm grasp of the initiative on the battlefield whether or not they are outnumbered.

Second, operational actions have become more precise. The greatest deterrent is no longer measured in formidable numbers but rather in the degree of informationization at the decision

making level, the command and communication systems that are relied upon, and their informatized weapons and equipment. With the progressive increase in transparency on the battlefield, operational actions are becoming more precise.

Third, attacking and defending actions have become integrated. The lines have blurred between several factors such as attacking and defending, front lines and depth, strategy and tactics, air and ground, civilian and military, and soldiers and civilians. The fluidity of the armed forces has increased greatly, and the operational battlefield can change at any time. All operational activities closely revolve around the intent to gain information supremacy. The operational space is arranged like a jigsaw pattern, forming an irregular, nonlinear front.

Fourth, operational space has expanded. In informatized operations, information space has become a critical realm for operational actions manifesting in electromagnetic space, network space, and psychological space. Electromagnetic space is the most intensive of future battlefield operation **countermeasures**. Network space is the result of the permeation of computer networks throughout the various layers, realms, and time segments of informatized operations. Psychology helps to **control** and determine how people think and act. Psychological warfare under conditions of informatized operations can cause an enemy to surrender with even no fighting at all. This has made for a new manifestation of information war space, namely psychological operations space. **Countermeasures** in psychological space in future wars, together with the struggle for psychological supremacy, will be even more fierce and widespread.

Fifth, **countermeasures** will become systematic. Informatized operations are **countermeasures** engaged in between systems and not a test of strength between individual battlefields or weapons. Information networks not only form tight systems composed of a spatial realm, an individual military service, the operational command for a department, weapons and equipment, and operational actions; they also turn the devices on the battlefield into a tight system where operational strength is dependent primarily upon the formation and function of the entire system. This system is interlaced in a criss-cross pattern, and it is agile in its response, has information sharing and confidentiality, is strong in anti-interference, has fewer layers of command, and can fully coordinate and exploit the prominent features and strategic functions of every level of personnel. It is an important support for informatized operations.

Sixth, operational means are diverse. Operational **countermeasures** for future informatized wars have brought forth higher standards, demands, and a greater diversity of operational measures. First, operational measures can perform both “soft” and “hard” attacks in a full-dimensional battlefield space. Second, there is a clear hierarchy of operational means, to include strategic means, combat means, and tactical means. Third, operational means have integrated multiple types of new technology, high technology weapons, and highly efficient tactics based upon information technology.

97. What Are the Principles of Informatized Operations?[588]

There are general principles to which informatized operations ought to conform.

First, the principle of breaking down the enemy’s combat abilities while maintaining one’s own combat abilities. In informatized operations the center of gravity for annihilating the enemy

involves the use of information attacks along with suppressing and interfering with the enemy's information systems, disrupting the enemy's psychological cognition, disrupting the enemy's operational systems, and breaking down the enemy's combat abilities. Preserving oneself refers to preserving one's strengths and the security and stable operation of one's information and information networks in order to maintain combat abilities.

Second, the principles of **comprehensive** integration and overall **countermeasures**. "Concentrating the best forces to annihilate every single one of the enemy" has always been the basic principle of the Chinese military. This type of concentration is manifested in a high degree of information-guided integration. Informatized operations are characterized by the overall **countermeasures** engaged in between the operational systems of both sides in a conflict. Information networks are used to link together operational forces into an integral operational system. The result is an overall coordinated movement that maximizes operational efficiency.

Third, the principles of hard and soft integration and attacking and defending nodes. Information attacks include electronic interference and firepower strikes on the enemy's information systems, the integration of tangible strikes and intangible destruction, the integration of direct action with indirect effects, the combination of the results occurring at the time of the strikes together with long term effects, and the maximization of interference, clampdowns, and cutting off the enemy's information activities. Protecting friendly systems, especially critical nodes is, in effect, "catching a whale with a minnow," i.e., accomplishing a great task with little effort by means of clever maneuvers.

Fourth, the principles of information sharing and self-coordination. Close coordination has always been an important guarantee for the success of an operation. However, coordination methods for informatized operations have developed into self-coordination, where action is primary. Network-based battlefield information systems enable information sharing and real-time perception of battlefield conditions. This enhances one's subjective initiative or creativity, self-coordination, and proactive coordination due to better understanding of a higher commander's intent.

Fifth, the principles of precision operations and **comprehensive** safeguards. With reliable intelligence information, informatized operations can realize precision of perception, precise transmissions, precise decision making, precise strikes, and precise movements. This establishes a material and technical basis for precision operations and attacks against critical nodes and important targets in hostile operational systems. In future wars, where **countermeasures** between systems will increase, precision strikes means taking out a whole area just by targeting one small part of it. Precision operations will become the goal and basic operational principle of every military.

Objective demands are such that logistics must respond quickly and **comprehensive** safeguards must be implemented to fully utilize information technology. Meticulous and precise planning and utilization of logistical safeguards provide troops with the right types, quantities, and quality of material and technical safeguards at the designated times and places, thereby increasing effectiveness. Chinese forces must move from quantity-based logistics to quality- and speed-based logistics in accordance with the principle of "reasonable sufficiency." Logistics need precision

safeguards suited to a time, place, and volume as a means of adapting to trends of future informatized operations.

Sixth, the “Three Negation” operational principles foster strengths while circumventing weaknesses. “No-contact operations” means utilizing superior firepower means to keep the enemy under a barrage of firepower and unable to form a threat. “Non-linear operations” means separating the enemy’s head from his tail while attacking his front lines, his depth, and his rear area. “Asymmetrical operations” means that “you conduct your war and I’ll conduct mine, but I can hit you while you cannot hit me.” One must use the right operational methods based on actual conditions to foster one’s strengths and circumvent one’s weaknesses and use one’s strengths to hit the enemy where he is weak.

98. What Are the New Changes to Informatized Operations?[589]

Recent regional wars have uncovered several changes in the development of informatized operations. Three of these changes are:

First, strike targets for informatized operations often come down to conducting operations in a specific order—psychological shock, material destruction, and physiological annihilation. In future informatized wars, information transmission and attack venues have changed war’s traditional emphasis on annihilating the enemy physically to shocking the enemy psychologically. Concentrating attacks on psychological targets, selectively destroying physical targets, annihilating a limited number of physiological targets, and complementing strikes on traditional targets with strikes on non-traditional targets is the new operational targeting selection process. Special actions such as warfare upon public opinion, psychological warfare, and legal warfare have attained a prominent function in war.

Second, informatized operations forces typically involve information concentration, firepower concentration, and troop concentration. Selected targets are then hit. Information guides the war: firepower is primary to the war: troops assist in the war. This is the new force utilization model. In Iraq the information aspect was activated before troops and weapons arrived. The US military’s first step was to deploy various types of satellites above the operational area, up to one hundred at a time, for a multi-layer reconnaissance and surveillance network composed of satellites, reconnaissance planes, and various types of early-warning and detection equipment. These systems monitored the battlefield and created favorable conditions for the concentration of firepower and troops.

Third, the informatized operations attack process involves the command and **control** level, the support level, and the combat level. Troops and weapons systems are the combat or base level, the material safeguard system is the support system or middle level, and the command and control system is called the **control** level or top level. Traditional wars typically start against the enemy’s operational troops in order to destroy the enemy’s effective strength. After that, the middle support level is broken down, followed by the annihilation of the command and control level to attain victory. In informatized operations, striking directly at the enemy’s command system has become a possibility. First, the enemy’s ability to organize operations is stripped, and then his base systems and material systems are disrupted. The enemy is unable to engage in war. Finally, Chinese forces strike at the enemy’s combat systems, a new operational objective. In informatized operations, the

base-middle-top level order of strikes has turned into top-middle-base.

99. What Systems Support Informatized Operations?[590]

At least four major systems will be needed for support in the informatized operations of the future.

First, integrated battlefield information reconnaissance systems. These systems implement informatized operations. During the war in Iraq, the US military used command center display monitors to observe conditions on the battlefield in real-time. They observed Iraqi tanks in motion, assault forces deployed in Baghdad, and Tomahawk cruise missiles. These systems enhanced both US military battlefield awareness and operational effectiveness.

Second, highly effective joint command and control systems. These systems are the key to implementing informatized operations since they allow commanders to remain in contact with their troops or individual soldiers, and they provide orders to operational troops in real-time which connects the force. This enables joint operations to conduct decentralized deployment, concentrated command, **comprehensive control**, and random strikes.

Third, intelligent precision strike systems. These systems conduct informatized operations. Imbedded information flows are connected together to form an attack network for intelligent weapons systems. The various weapons platforms and firepower units for different services are the equivalent of a node in the network. Battlefield information can be shared immediately. When informatized equipment, command and control, and operations platforms are integrated and connected on the battlefield, an intelligent weapons system firepower force develops.

Fourth, precision operational support and safeguard systems. An integrated precision support and safeguard network helps implement informatized operations. The desire is to change the traditional model for logistical safeguards and fuse elements such as information logistics and transfers together. This will provide operational troops with **comprehensive** logistical support safeguards featuring the right quantities in the right place at the right time.

Information Technology

112. What Are Information **Countermeasure** Technologies?[591]

Information **countermeasures** are the disruption or destruction of the enemy information systems' normal acquisition of information while ensuring the normal function of friendly abilities to acquire, transmit, process, and use information. Information **countermeasure** technologies refer to the various technologies to conduct information **countermeasures** such as information attack and defense technologies. They form **comprehensive** application technologies and are the manifestation of information operations technical level.

The development of information **countermeasure** technologies will result in informatized operations becoming a type of systematic **countermeasure** action. The use of a new information technology in war necessarily results in the creation of a new **countermeasure** technology which then drives the further development of said information technology. The result of the interaction of these two aspects (the dialectic at work) has driven the development of information

countermeasure technology and the patterns of informatized war.

Information **countermeasure** technologies are the **comprehensive** applications of many information operations technologies. Information **countermeasures** are of key significance to the **comprehensive** improvement of informatized operations technologies. The latter places new demands upon information **countermeasure** technologies to include the complete coverage of frequency, round-the-clock coverage of time, multi-dimensionality in the area of space, and **comprehensiveness** when it comes to methods.

118. What Are **Comprehensive** Integration Technologies?[592]

Comprehensive integration is the organic combination of several units for systems that were not connected (or not closely connected) to form a new coordinated and optimized system. **Comprehensive** integration includes system engineering, software integration, demonstrations for **comprehensive** integration, and scientific planning and management. **Comprehensive** integration technologies are engineering technologies and an art. They are important ways and means to transform engineering technologies into combat capabilities. The essence of **comprehensive** integration is the integration of scientific theory with experiential knowledge, the integration of human thinking with computer analysis, and the integration of individual judgment with the group to exploit the overall advantages of **comprehensive** systems. The goal is a major system with a high degree of antidestruction capability that is interoperable and works in real-time.

The use of **comprehensive** integration technologies in the military enhances the operational efficiency of weapons and equipment and the overall operational caliber of troops. As the informatized operations component takes over, it will trigger the launch of systematic **comprehensive** integration across the board and provide embryonic form to informatized operational systems. There will be revolutionary changes to operational means and methods during this stage.

Comprehensive integration technologies have five major linked aspects:

- First, hardware integration, the integration of weapons platforms, various types of information operations hardware, and the subsystems they make, all supported by computer networks. Hardware integration is the foundation for **comprehensive** integration.
- Second, software integration, the integration of all system software, tools software, and application software in the system. The major software integration issue is that of ports which work between heterogeneous software. The various kinds of software must conform to the requirements for international standards and open-source software as much as possible. At times, it is necessary to formulate unified standards and regulations to enforce this.
- Third, data and information integration, the rational unified planning and arrangement of data to avoid unnecessary or harmful redundancy and to provide consistent and transparent interfaces for information sharing.
- Fourth, function integration, the coordination of the functional aspects of command, **control**, and management of operational systems and their integration into an advanced

operational function.

- Fifth, the integration of individuals and organizations, viewing individuals and organizations as integral components in a system and as the most critical and active elements in the system to achieve coordination. The coordination of individuals and organizations with other components of the system results in a system maximizing its overall effectiveness.

123. What Are Anti-Information Strategy Technologies?[593]

“Anti-information strategy technologies” means that when targeting weaknesses in the enemy’s operational command information platforms, great efforts go into developing interference with, obstructions of, and disruptions of information transmission and destroying technology related to the command chain as a means of creating favorable conditions for gaining information supremacy and winning victory by stealth.

While information advantages are the equivalent of the functional advantages of “ $1 + 1 > 2$,” a serious structural defect is the equivalent of “ $100 - 1 < 99$,” a congenital deficiency which is difficult to eliminate. As such, once the weaker side trains its sights on the weaknesses in the enemy’s system and attacks them effectively, it just may snatch victory from the jaws of defeat. Dialectically speaking, information supremacy leads to the defeat of the enemy, but it may also be a “weak” supremacy at the same time. Anti-information strategy technologies can make use of this “weakness” in the supremacy to find a turning point for **countermeasures**. Contests on the battlefield are vastly different from those in sports as there are no rules and most any means can be used. With anti-information technologies Chinese forces can defeat a stronger opponent and make up for some shortcomings.

Foreign military experts believe that new anti-information strategy technologies have functioned “like a sharp sword to slice information strategies in two.” Possessing them is equivalent to a new type of nuclear weapon that can become a wild card for the weak when they employ information **countermeasures** as a form of strategic containment. The broad use of new anti-information strategy technologies will create enormous capacities to break down an enemy and huge advantages for producing effective and formidable information deterrence capabilities. A foreign expert in military information warfare noted that it is very difficult to establish information ‘TMDs’ in information space. Someone always seems to find a way to get into information systems and make you deaf, dumb, blind, and weak in useful intelligence.

126. What Are the New Technologies for Intelligence Reconnaissance?[594]

Intelligence reconnaissance systems technologies include signal reconnaissance for spread spectrum communications, software-based detection systems, spatial spectrum estimation for direction finding, stratospheric balloon-borne reconnaissance, signal fingerprint reconnaissance, remote battlefield reconnaissance radar, and **comprehensive** intelligence reconnaissance. Only signal reconnaissance, remote battlefield reconnaissance, and **comprehensive** intelligence reconnaissance are discussed here.

Signal reconnaissance technologies for spread spectrum communications include capturing and de hopping frequency-hopping communications signals. There are basically three procedures for intercepting frequency-hopping signals: capturing, sorting, and de hopping. Owing to the fact

that frequency-hopping signals hop quickly, great demands are placed on the search speed of the receiver. Present signal channel receivers and digital receivers using fast fourier transform (FFT) technology search quickly and retain communication information. The frequency, time, and spatial features make it possible to sort the frequency group of the frequency-hopping network platform for fixed-hopping speeds or variable hopping speeds. Cache and splicing techniques work to dehop the frequency-hopping signal. After dehopping, the frequency-hopping signal becomes the same as regular signals, where demodulation and decoding can produce a communication signal.

The second type of signal reconnaissance for spread spectrum communications is to detect and despread direct-sequence spread spectrum communication signals. The power spectrum density for direct-sequence spread spectrum communication signals is low making it difficult to detect their presence using conventional reconnaissance receivers. The premise of despreading is in detecting the presence of direct-sequence spread spectrum signals and in estimating their parameters. Feasible and effective methods include energy detection, the inverse-spectrum method, autocorrelation detection, and cycle-spectrum density detection. All of these methods have their good and bad points. The energy detection method is quick, but does not make use of the special characteristics of spread spectrum code which decreases detection. The implied processing in the inverse-spectrum method can increase the signal-to-noise ratio for output, but detection is slow. Cycle-spectrum density detection can detect various characteristic parameters for signals **comprehensively** and accurately, but at low speed. Autocorrelation detection can be used once the detailed structure (variable patterns such as frequency, phase, and code width) of the enemy's spread-spectrum communication signals is known. Despreading is fast and highly effective, but the engineering is still very difficult.

Remote battlefield reconnaissance radar is a type of detection sensor installed on an airborne platform, and works by looking down. It can detect, position, and recognize distant (100–200 kilometers) moving targets, including targets on land, sea, and in the air. It can be used as a synthetic aperture to acquire radar images from objects on the ground, and it can monitor fixed military targets. Real-time processing turns into war zone intelligence. Remote battlefield reconnaissance radar can work in harsh climate condition. It combines adaptive moving target detection (AMTD) and synthetic aperture radar to enable reconnaissance of live and fixed targets.

Comprehensive intelligence reconnaissance refers to the use of rational system structures since reconnaissance sensors are connected with multiple reconnaissance platforms to form an organic entity which fuses intelligence to produce prompt, accurate, and complete intelligence. In **comprehensive** intelligence reconnaissance systems the information comes from multiple sensors and can be both complementary and redundant. Information fusing procedures such as detection, connection, correlation, amalgamation, the assessment of target recognition, posture description, sensor management, and database processing can incrementally increase the degree of abstraction in primary information so that more valuable intelligence is the result. **Comprehensive** intelligence reconnaissance systems have large coverage in terms of time-space and the electromagnetic spectrum, strong detection capabilities, good accuracy in target positioning and recognition, strong timeliness and predictive nature of the intelligence gathered, good system for errors, and multiple sensors and platforms working together.

127. What Are the New Technologies for Early Warning Detection?[595]

Early warning detection systems include two types: information fusion technology in multisensors in early warning systems and target positioning technology in passive detection systems.

129. What Are the Principles for the Function of Information Warfare?[596]

Basic principles for the function of information warfare follow.

First, the influence and impact of information upon cognitive systems will cause personnel on the battlefield to make different decisions and take different actions. Information keeps the basis for decisions and actions on the battlefield from becoming aimless and random. This is a basic principle of information warfare.

The influence of information upon cognitive systems is manifested in three ways. First, information can be true or false. It can steer a commander into making the right or wrong decision or action. Second, the complexity of information makes it difficult for commanders to make quick decisions. The simpler information is, the easier it is for people to make decisions and take actions. Information volumes in informatized wars are enormous. This makes it difficult to make high quality decisions in a limited amount of time and to coordinate actions. Third, the variability of information can result in commanders missing prime opportunities because they are too busy or acting in haste. Variable operational means, fast-changing operational rhythms, and shifts between attacking and defending all present serious challenges to those processing information.

Second, the effect information has upon materials and energy enhances one's own combat capabilities and weakens those of the enemy. How much information can be **controlled**, how precise it is, and how free-flowing regulates action on materials, energy, and weapons systems to varying degrees. The information struggle enhances or reduces the **control**, free flow, or precision of information. This has become one of the active principles of information warfare.

The regulating action information exerts upon materials and energy is manifested in two areas. First, the **control** and precision of information can act to distribute materials and energy. How they are distributed and where they are distributed are two aspects which are **controlled** by information. The distribution of materials and energy must develop in the direction of meeting operational goals. Second, the free flow of information can help guide the flow of materials and energy. Information is an effective "carrier" of materials and energy and can act as an intermediary for the fusion and distribution of materials and energy. On the battlefield, the side with information supremacy will have stronger combat capabilities and a more formidable space for initiative.

Informationized Armed Forces

141. What Are Electronic Warfare Units?[597]

Troops conducting electronic **countermeasure** reconnaissance and electronic interference are known as electronic **countermeasure** units. They are divided into communications **countermeasures** units and radar **countermeasures** units, according to their targets. Electronic warfare units exist in each military service. Ground electronic **countermeasure** units are organized into regiments, battalions, and companies, and even brigades in some countries. Electronic **countermeasure** air force units are organized into companies and squadrons. Units on

naval ships are organized into electronic warfare ships.

Electronic warfare units' primary tasks are to:

- Conduct electronic **countermeasure** reconnaissance
- Acquire information such as the technical parameters for the enemy's electromagnetic radiation signals and the type and configuration of their equipment
- Interfere with targets
- Weaken or destroy the enemy's electronic equipment and weapons systems
- Support and coordinate with the combat actions of operations units
- Create favorable conditions for victory in combat.

142. What Are Network Warfare Units?[598]

Network warfare units are dedicated units that use information technology to conduct attacks and defensive operations throughout network space against computers and computer networks. Dai believes that the United States and the United Kingdom have begun setting up network warfare units while Russia, Japan, South Korea, and India are looking to set up dedicated network warfare units in the future.

The structural organization of network warfare units is based upon the basic operational principle of gaining the initiative in warfare and destroying the enemy's intentions to act, thus **controlling** how a war proceeds. Network warfare units analyze and predict based on how events look in general. Units must engage in precise communication and coordination to promptly and accurately make the right analysis of battlefield conditions. Judging the enemy's posture and intent helps to make actions more effective. Their basic function is to gain information supremacy.

In future information wars, Dai states that network warfare units will take orders directly from each of the military services/command units and will be tasked with safeguarding the secure operation of the strategic, combat, and tactical computer systems and networks for the various armed forces. "Tangible tasks" will include computer security firewalls, antipiracy, defense against attacks, and guarding against static and security electromagnetic radiation leaks. "Intangible tasks" include reconnaissance, defense, and antispam and antivirus protection that safeguards network security.

152. What Are the Trends in the Informatization of Military Strategy?[599]

Just as the nuclear trend in military strategy appeared with the advent of nuclear weapons, modern day military strategy concepts are centered on information. Dai notes that military leaders and theorists in some countries are currently using the following jargon: information supremacy, information deterrence, information monopoly, information attack, information defense, information threat, information umbrella, and information safeguards. These terms were first used with nuclear issues.

Of the terms given above, information deterrence, information umbrella and information safeguards are more frequently used. Dai states that Professor Roger Barnett, of the United States Naval Academy, asserts that the foundation for information deterrence is in having formidable information attack capabilities. The threat of an information attack is similar to that of a nuclear

attack in that it can paralyze cities, regions, and industry. Dai also states that William Owens, former vice-chairman of the US Joint Chiefs of Staff, believes that the function of the information umbrella is, in a significant sense, greater than that of the nuclear umbrella since it can be used in peacetime. During times of war, it allows the US to provide strategic, combat, or tactical information support to its allies, thus amplifying combat capabilities.

Informationization of the Armed Forces

157. What Are the Main Characteristics of the Informatization of China's Military?[600]

There are five main aspects to the informatization of the military with Chinese characteristics. First, there are strategic objective limitations. The informatization of the military with Chinese characteristics is an essential expression of a military strategy of vigorous defense. The goal is to enhance defensive capabilities under conditions of informatized war to safeguard the nation's security and development. Dai states that this is an essential difference between China and Western countries.

Second, there is unification of the organization of leadership. Dai believes that the absolute leadership of the Party over the armed forces is an excellent tradition in the Chinese military and offers a unique political advantage, a military revolution led by the Communist Party of China. It is a top-down approach, unified and progressive. It is a fundamental guarantee that informatization proceeds smoothly in terms of organization and the system.

Third, there is the dual nature of the environment of the revolution. The informatization of the Chinese military is proceeding in an environment where the transformation of the military and the socialist economy are occurring almost simultaneously. This creates a "dual revolution." The country must perform **comprehensive** planning for the social revolution happening across the entire country. Military informatization must be incorporated and in step with political, social, and economic reforms. At the same time, the informatization of the military cannot overstep the capacity of the social reform to accept it.

Fourth, there is a difference in foundations for development. The informatization of the military with Chinese characteristics is still comparatively weak. In essence, a revolution with strategic directorial thought leading the way is driving successive revolutions in other important elements of the military realm such as for military technology, weapons, and equipment.

Fifth, there is the factor of leapfrog development. The Chinese military is undergoing reform and moving toward the era of informatized war on the foundation of only partial mechanization. The informatization of the Chinese military must leapfrog over one or several of the developmental stages that the West experienced.

158. What Are the Key Elements Promoting the Informatization of China's Military?[601]

Military informatization touches upon many areas. There are four key elements promoting military informatization at present and into the future.

- First, the establishment of new military thought. New military thought has hastened innovation.

- Second, enhancing independent innovation in the area of science. Advanced scientific technology drives the military revolution.
- Third, holding firm to the idea that people are the foundation of the buildup of the military. China must find the right personnel, strategy, and engineering. Having the right military commanders, planners, scientists, technical experts, and soldiers is critical.
- Fourth, strengthening concentrated and unified leadership. The unified leadership of the Central Committee of the Party and the Central Military Commission is supporting the following: the unified planning of programs, principles, policies, and procedures for the informatization of the military to ensure military and political coordination; maintaining the special characteristics of the Chinese military; learning from the experiences of foreign militaries; and reform and stability. The goal is to enhance informatized operations capabilities and heighten the scientific and democratic aspects of policy-making.

160. How Do We Make Full Use of Civilian Information Resources to Raise the Informatization Level of China's Military?[602]

China's military needs to hold fast to the principle of integrating military and civilian personnel and integrating peace and war. This particularly applies to the use of reserve forces. China must incorporate the buildup of civilian information systems into its overall plans. Civilian network distribution should consider wartime requirements, and technical systems should be compatible with the military. Information reserve forces must be built up and given a prominent position in national defense mobilization. High-level information technology personnel must be prepared and methods to appropriate civilian information systems defined. China must absorb information reserve forces into combat training and exercises, put research into the characteristics and patterns of operations conducted under informatized conditions, and conduct drills for operational tactics under informatized conditions.

161. What Are the Basic Elements of the Informatization Buildup of China's Military?[603]

The informatization buildup of China's military must grasp foundational elements such as information technology applications, the development and utilization of military information resources, the buildup of military information networks, training for dedicated information personnel in the military, and the policies, laws, regulations, and standardization of military informatization.

First, information technology applications. China must adopt methods to enhance the informatization of single weapons platforms to increase their operational efficiency. The systematic nature of information technology allows China to adopt **comprehensive** integration to enhance the operational capabilities for weapons and equipment. A "one-stop method" in the development of weapons and equipment allows China to skip over mechanization and move directly to informatization. Studying advanced technology of foreign militaries and adopting some items from the civilian sector will accelerate informatization's progress in weapons and equipment. The virtual nature of information technology allows for simulations that imitate weapons and equipment and shorten the research and development stage.

Second, the development and utilization of military information resources. The direct

objective of military informatization is to use more information resources and to optimize the coordination and utilization of material and energy resources. This speeds the buildup of the armed forces. The development and utilization of military information is the core task in the buildup of military informatization.

Third, the buildup of military information networks. Military information networks are at the core of the buildup of informatization. The construction of advanced information networks allows the military to fully exploit the overall effect of the informatization of the armed forces.

Fourth, the development of professional personnel in the area of military information. Information technology and information resources require people for research, development, and innovation. Fostering professional personnel in the area of information will have a decisive impact on the speed and quality of the progress of the informatized armed forces.

Fifth, the formulation of policies, laws, regulations, and standards for military informatization. These elements work to standardize and coordinate relationships among the various elements in informatization and to guide their implementation. They assure the fast, continuous, orderly, and sound development of military informatization. The policies, laws, regulations, and standards for military informatization must be scientific, advanced, practical, and operational to assure a swift, orderly, and sound buildup.

164. How Do We Understand the System of Regulations and Standards That Must Be Perfected in Promoting the Informatization Buildup of China's Military?[604]

The system of policies, laws, regulations, and technical standards for informatization regulates the informatization buildup and is a guarantee for a quick and sound resolution of the issue. By 2002 the State Council and various ministries had enacted over thirty laws, regulations, policies, and technical standards for informatization. Various levels of local government enacted specific policies and standards, and a system of laws and regulations were formed at the national and local levels to unify regulations and technical standards for informatization.

At present there is still no conventional system of policies, laws, regulations, and technical standards for the informatization buildup of China's military. A related system of laws, regulations, and standards needs to be further perfected under the unified national regulations.

First, the Central Military Commission and the General Headquarters of the PLA must develop a system of policies, laws, and regulations to develop the informatization buildup of China's military. Specific laws, regulations, and doctrine regarding the acquisition, exchange, and use of military information must be revised and perfected along with supporting management mechanisms and rules. Information security for national defense and the operation of information network security requires that China must focus on the confidentiality, integrity, serviceability, reliability, and **controllability** of information security laws and regulations. A legal and regulatory framework allows China to manage and ensure military information security.

Second, China must accelerate the formation of a system of technical standards for military informatization. The critical topics are the fusion and integration, **comprehensive** operation, and secure defense of military information systems. The formulation of standardization policies and

certification systems must be compatible with national standards.

165. What Is Top-Down Design?[\[605\]](#)

As people pay more attention to relationships, a shift in the center of gravity will occur to a high-level design with emphasis on a system of matters and things. This is how top-down design was created. Top-down design refers to planning for the buildup and development of the informatization of the armed forces. It is a strategic objective design featured by macro transformation and a long-term nature. It is essentially about designing the directions, objectives, and paths for military development. Scientific top-down design fuses scientific technology and military thought together into a whole, can fuse strategy and tactics together, and can fuse space and time together to form an integrated military system. Top-down design is macro, authoritative, stratified, time-sensitive and targeted.

Top-down design primarily entails the following:

- The goals, paths, and developmental steps for the informatization buildup of the armed forces
- The systems of command organization, expert consultants, and examinations and estimations for the informatization buildup of the armed forces
- The informatization of weapons and equipment systems
- The informatization of battlefield systems
- The informatization of the structure and structural organization of the military
- The developmental planning and standards for the informatization of personnel teams and operational theory
- The schemes, policies, laws, regulations, technical systems, technical standards, and systems of evaluation for the informatization buildup of the armed forces.

Top-down design takes into consideration the current conditions of the country and the military and military expenditures. When it comes to issues affecting the whole, such as the structure of the military and its structural organization, the informatization of weapons, equipment, the battlefield, and the informatization of personnel teams, Chinese forces must proactively coordinate with related areas while either commissioning others to do work or work cooperatively with them.

166. How Do We Properly Make a Top-Down Design in the Informatization of China's Military?[\[606\]](#)

The Central Committee of the Communist Party and the State Council take a strategic perspective of the nation's development. They place great importance on macro decision making and policy adjustments for the national development of informatization. They have enacted a series of plans and programs to incorporate informatization into the master plan for national development allowing it to develop in concert with industrialization. In April of 1997, the State Council enacted the "Ninth Five-Year Plan for National Informatization and Far-Reaching Objectives for 2010," along with the "Tenth Five-Year Special Plan for National Informatization." These plans have elucidated the definition and content of what national informatization entails, have determined its systematic structure and established its basic targets, developmental goals, elements of the buildup, and specific tasks to form a more complete top-down design.

Three aspects of the top-down design of the informatization buildup of China's military must be mastered. First, scientific strategies must be developed. The developmental strategies for the informatization of China's military should have as their basis the strategic programs drawn up by the Central Military Commission, and they should be guided by the developmental strategies for national informatization. The focus is on objective factors such as the existing scientific and technological strengths in national defense, military expenditures, and current conditions of the buildup of the armed forces.

Second, a systematic scientific structure must be established that is assured by laws and regulations, policies, doctrines, and technical standards for informatization, with the development of information resources as the objective. The goal is for military personnel to be knowledge-based, to have intelligent weapons and equipment, to have a network-based battlefield environment, scientific structural organizations, epochal military theory, and informatized military activities. China wants network platforms integrated for the three armed services and for strategy, combat, and tactics. This will bring about effective, secure, and reliable transmission of operational information for early warning detection, intelligence reconnaissance, command and control, electronic **countermeasures**, the operation of weapons and equipment, the implementation of operations, and the perception of battlefield posture.

Third, Chinese forces need to choose the right path of development. China must expand investment in the military's information infrastructure, to include C4ISR systems and data link equipment. China's military must give prominence to resolving system integration problems; interlinking and **controllability** problems; and advancing military information networks toward the development of **comprehensive**, wide band, and integrated military information base networks. Weapons systems construction must be sped up and work focused on informatized weapons systems which integrate multiple dimensions of space.

Battlefield Information Systems

256. What Is C4IKSR?[607]

C4IKSR is the abbreviation for a system with command, control, communications, computer, intelligence, strike, reconnaissance, and surveillance capabilities. The elements are integrated into one network when using the C4IKSR system. This makes for automated **control** of early warning detection, intelligence reconnaissance, surveillance, identification friend or foe, tracking, and electronic **countermeasures** on various enemy targets right up to the hit, along with a seamless connection for the entire operational flow involving reconnaissance, decision making, kill, and loss evaluation. Commanders initiate operational actions and **control** and manipulate remote precision-guided weapons systems thus expanding the range of command activities.

Informationized Operations Command

270. What Are the New Changes in a Comparison of Operational Command under Informatized Conditions and Traditional Operational Command?[608]

Informatized war exhibits many changes which have led to many changes in operational

command.

First, precision command has become the main trend. Precision command exploits the advantages in the integration of man and machine by allowing command personnel to integrate their subjective initiative with precision quantitative calculations and analysis. Precision command entails concise decision making, seamless planning, and **control**. Precision **control** emphasizes creating overall momentum in strategy and combat and focuses upon grasping specific operational actions by emphasizing a shift from the previous general strikes and **control** in a given area to the precision strikes and **control** on a “point.”

Second, nonprogrammed command is becoming more prominent. Informatized weapons have rigorous technical standards and workflows which is why the armed forces have become even more programmed. Yet the development of command information systems has created conditions for nonprogrammed command. The seamless integration of information collection networks, information transmission networks, and information processing networks makes for a high degree of transparency on the battlefield where posture is shared and actions are self-synchronized. Commanders can implement **stratagems**, demonstrate their talents, and engage in daring innovation.

Third, concentrated and decentralized command will interact closely. On the network-based battlefield, every operational unit and soldier will have advanced information equipment allowing for smooth exchanges and communication among them. In future informatized war, operational units can participate in command activities formerly limited to command bodies. Decentralized command will increase leading to a higher degree of interaction between concentrated and decentralized command.

Fourth, the status of real-time **control** will continue to increase. Operational command is evolving from aggregate planning to aggregate **control**. During the war in Iraq, US military planes were equipped with systems for receiving intelligence rapidly, and about two-thirds of the planes were not given explicit tasks to perform before takeoff. Instead, they waited in the air above the battlefield for real-time operational intelligence, and then launched their strikes.

272. What Are the Basic Demands of Informatized Operations on Organizational Command?[609]

First, operational effectiveness needs to be enhanced. Informatized operational space has expanded, time has become concentrated, operations have sped up, and attacking and defensive actions have become very fast. Chinese forces must do their best to shorten the decision making cycle and keep the emphasis on being “fast” from beginning to end. Being fast is the very soul of operational command. Initiative is won and advantages are gained by being fast.

Second, command needs to be implemented accurately. Information deception and interference, the coexistence of real and false information, the unprecedented complexity of the information environment, and the changes occurring from minute to minute result in the complexity of the information environment and difficulty to conduct accurate operations. This all requires that commanders be extremely good at sensing the larger picture from small clues, be apt at discovering things promptly and capturing the smallest of irregularities on the battlefield, and be good at grasping the posture of the entire battlefield and predicting how it will progress and

change. They need to fully exploit the intelligence and cleverness of strategists, along with the systems which assist in decision making, to conduct accurate operations.

Third, command needs to be flexible. On the informatized battlefield there is no tangible dividing line between the two sides in a conflict. There is a lot of movement, and battlefield posture can change in an instant. Flexible command and flexible coordination of command bodies are required. Commanders need to be good at making use of tactics and troops, adjusting deployments, changing attack methods in a timely manner, and turning passivity into initiative under changing conditions.

Fourth, the security of command systems must be protected. Operational command systems are the nerve centers for action and troop actions descend into chaos when they are broken. This is why the primary objective for both sides in a conflict is to strike at the enemy's command system. There is an enormous threat to the survival of command system making security for them especially critical.

273. What Elements Should Be **Controlled** to Improve Command Effectiveness under Informatized Conditions?[610]

The following four elements should be **controlled** in order to improve operations conducted under informatized conditions

First, information transmission. It is imperative that the transmission, processing, exchange, and acquisition of intelligence are prompt, accurate, continuous, and reliable, and that computer data, digital voice information, video, and static images can be transmitted promptly. Good anti-interference, anti-acquisition, reliable network and information security, and confidentiality are essential as well to improve the integration of **comprehensive** command systems.

Second, information resource sharing. The goal of information resource sharing is for military organizations and individuals within a prescribed domain to use information resources as much as possible, to coordinate information resources in terms of timeliness and quantity to provide a rational information layout, and to satisfy user demands for information to the greatest extent possible.

Third, command and decision making. Decision making support systems connect two or more command bodies using visual communication equipment. Electronic facsimile technology can organize meetings and enable decision making. Each person's plans (developed using his or her computer or terminal within the same command post) are combined and produced for discussion. A large screen display shows the plans of the individual decision makers, and the results are provided as statistical data. This method connects command posts which are far away using computer networks, telephone networks, electronic blackboards, video, and large screen displays. This is the modern way of making decisions collectively.

Fourth, lateral integrated operations. The informatized battlefield demands that command and control are highly concentrated and integrated with each other. However, the integration of command can only occur when technology is integrated. As such, elements such as reconnaissance, command and control, communications, strikes, and damage assessment must be integrated into a

whole by means of information networks and systems in order for effect real-time target discovery, real-time command, real-time strikes, and real-time safeguards.

Joint Operations

332. What Are the New Changes in Information Operations under Informatized Conditions?[611]

Information operations began with electronic warfare. In wars during the information era, information operations will be reflected in integrated joint information operations. These are, in effect, the total intentions of integrated joint operations under informatized conditions, and they involve the unified overall goals of information operations. Each of the elements of information operations are fused together, and they are characterized by the combined actions of dedicated information operations forces linked together with nondedicated information operations forces. Integration refers to information operations units with similar functions coming together to form a single system on the basis of information technology, particularly network technology, to achieve information sharing and thus enhance the overall capabilities for information operations.

The term “joint” here refers to the fusion of the various elements in information operations as a means of exploiting their overall actions. This is the premise and foundation of integration. Information operations are viewed as integrated joint actions between the various military services. It is important to keep the different elements in harmony with one another and work toward total synthesis. This improves the effectiveness of information operations.

335. What Is System Sabotage Warfare?[612]

The basic characteristics of informatized wars are that they are guided by information and that they consist of two systems fighting each other. This is why system sabotage is so important as it is the decisive mechanism of informatized operations, and it is the basic path to victory in informatized wars.

The key point to system sabotage is in “gaining **control**, precision strikes for maximum damage, and paralyzing the enemy to subjugate his will.” This primarily entails using asymmetrical operations where the emphasis is on the “destruction” part of the equation. Methods to attack weaknesses in a system include blocking network connections, breaking down the system architecture, and lowering operational effectiveness.

This is a key paragraph in Dai’s book. He notes that to make system sabotage effective, there needs to be a basic mode of thinking where the Chinese “destroy before conducting war, using destruction to aid in the fight.” This is because, under informatized conditions, the core elements and mechanisms for victory in war have undergone critical changes. There are significant differences in the procedures and the center of gravity for operations in comparison with how they were in the era of mechanized war. Not destroying the material and technical foundation upon which a system of integrated operations and operational actions depends, i.e. the network-based information system, makes it impossible to convert negatives into positives on the battlefield. Obviously, conducting system sabotage requires an emphasis on destroying the network first before engaging in war.

For “destruction,” this refers to concentrated and continuous strikes on perception and

information transmission systems on the battlefield. Implementing strikes where Chinese forces “kill two birds with one stone” means cutting off the “seamless link between sensors and launchers” to greatly hamper reconnaissance and detection capabilities, rapid response capabilities, and precision-strike capabilities in an integrated operational system, thus creating the opportunity for continuous operations and the chance to “divide and rule.” When it comes to “combat,” this primarily refers to the favorable conditions in war for reducing the effectiveness of an operational system by conducting long range precision-strikes as the primary means of nonlinear, noncombat operations. Continued strikes on weak points break down an enemy’s operational actions, shatter his operational intentions and shake his will to resist. Of course, there is combat occurring during destruction, and vice versa so the two are connected but the focus and aim are different.

336. What Is Network-Centric Warfare?[613]

Dai states that the concept of network-centric warfare was first proposed by the US military. He adds that the US believes it will be one of their main forms of operations in the future. Dai noted that the US military definition of network-centric warfare is as follows: “Network-centric warfare” is a military action conducted by a network-based unit and occurs in the physical realm, information realm, and cognitive realm concurrently and between them. The physical realm refers to the tangible realm that includes weapons and equipment (physical networks, communication networks, and the physical space in which war occurs). Here network-based units conduct operations. The information realm is the realm in which information is created, gathered, processed, transmitted, and shared. The cognitive realm refers to the consciousness, thinking, and psychology of operations personnel. This includes their perceptions, understandings, beliefs, and values, along with the decisions they make based upon them. They also involve the abilities of military leaders, the morale and cohesiveness of troops, the caliber of training, experience in combat, the ability to perceive posture, and public opinion.

Simply put, network-centric warfare refers to operations in which computer networks are used to conduct the unified command of a military unit. The operational units in network-centric warfare are all network-based, and information superiority is converted into operational action superiority so that the various units collectively **control** and are aware of battlefield posture. This allows for **control** over battlefield posture, quicker decision making, fewer errors in decision making, faster command, and better coordinated operations with which to engage in enemy strikes.

To conduct network-centric warfare requires a network-based armed forces. The four key elements of network-centric warfare are as follows: First, the “information structure,” meaning a system in which all of the sensors are connected to a network and the system conducts data fusion and information management. Second, “operational space perception.” The establishment of an “information structure” makes operational tasks, actions, and terrain transparent so that individual units can perceive the ever-changing battlefield posture at the same time. Third, “real-time coordinated actions.” It is important that one’s own operational actions are always one step ahead of the enemy and one has the initiative. Individual units can intuitively execute operational orders. Fourth, the “final effect” of the information structure, operational space perception, and actions coordinated in real-time is that the rhythm of operations is accelerated, responsiveness is strong, the risk in operations is reduced, there is a lower cost to operations (primarily in terms of casualties), and the effectiveness of operations is increased.

There are several special features to network-centric warfare. First, it is significantly proactive and caused the US to seek **comprehensive** superiority. Second, the flow of information has replaced the traditional flow of human resources and materials thus reducing operational risk and consumption while strengthening combat capabilities. Third, network integration warfare will bring new changes to the structural organization of the military and to weapons and equipment. A whole host of new information weapons systems are going to appear. Fourth, bringing network integration warfare to fruition is a comparatively longer process both theoretically and practically.

Network-centric warfare will result in five operational advantages. First, it will make **comprehensive** use of decentralized military forces. Second, it lowers the risk of operations. The enemy will not be presented with high-value targets thus reducing the risk in operations. Third, it will reduce the strain on logistics. The workload for medical services and material transport and reserve supplies of fuel and munitions will be greatly reduced. Fourth, military units will have a thorough grasp of the situation they are in. Fifth, military units will be able to maximize operational effectiveness. The various operational units in the operational space will be connected by networks into an integrated whole.

Network-centric warfare has some inherent drawbacks. First, those engaged in it need to set up an information-gathering system on an enormous scale. This includes reconnaissance satellites, for example. This means that substantial financial resources are required. Second, information quantities are increased, which places greater demands on the various levels of command. Third, it relies too much on computer systems which gives the enemy an effective target.

339. What Are Asymmetrical Operations?[614]

Asymmetrical operations refer to operational actions by two sides in a conflict which are asymmetrical in terms of their force. Asymmetrical operations use the terminology of natural science to express the concept of the relative relationship between one's own force and that of the enemy, and the antithesis is asymmetrical operations. Asymmetrical operations can refer to a conflict between two forces of different types, such as between an air force and a naval force, an air force and a ground force, or a ground force against an air force and a naval force. Asymmetric operations leverage the objective difference between different types of forces as a means of using one's advantages to attack an enemy's weaknesses and preserving one's own initiative. [Author's note: this definition of asymmetrical operations is slightly different than the definition offered in the next chapter, and vastly different from the definition offered by author Kang Hengzhen, a Senior Colonel and research fellow at General Staff Headquarters, in a 2002 issue of China Military Science. Kang defined asymmetry as "abnormal logic bringing together two sides that are pitted one against the other. It radiates the dialectic with 12 crafty tactics." Thus it appears that there remains wide divergence in what the term actually means.]

344. What Is "Threefold Warfare?"[615]

"Threefold warfare" is a completely new concept proposed by the Chinese military as a lesson learned from watching US activities during and after the 2003 intervention into Iraq. The three elements are warfare of public opinion, psychological warfare, and law warfare. They encompass operations conducted on the basis of news, public opinion, human psychology, and law. "Threefold warfare" is a **comprehensive** concept in which the country and the armed forces,

guided by military strategy, integrate various societal resources to win the political initiative and the psychological advantage. Attacking and counterattacking are the basic forms of combat. The goals are to fortify oneself as much as possible, win friends, and break down the enemy. The main entities in “threefold warfare” are the state and the military. It is a form of special operations. It features the ability to outflank opponents and can be used indirectly as opposed to weapon power. Psychological warfare is the core of threefold warfare.

345. What Is “Psychological Warfare?”[\[616\]](#)

Psychological warfare refers to **countermeasure** activities conducted in the spiritual and psychological realm by two sides in a conflict. It is backed up by actual or potential military force. Weapons are various forms of information media and the combined use of various communication methods. Psychological factors exert their influence, restricting and altering the enemy’s thinking, feelings, and behavior, while increasing and solidifying the psychology on one’s own side.

Modern conflicts which erupted in the Gulf, Kosovo, Chechnya, and Iraq saw the use of multiple types of psychological warfare. In particular, the US military conducted omnidirectional psychological warfare against the Iraqi military during the war in Iraq, making it fully deserving of the epithet “the second battlefield.”

There are broad and narrow definitions for psychological warfare. In the broad sense, psychological warfare includes propaganda warfare, news warfare, and media warfare. In the narrow sense, psychological warfare refers only to the impact and the awe inflicted on enemy forces psychologically on the battlefield. The requirements for psychological warfare in the broad sense are as follows: you (the Chinese) need to attack the legality and reputation of the sovereignty and political systems of the enemy; you need to mobilize the people to support military, paramilitary, security, and intelligence activities; you need to mobilize the people to support political, societal, and economic plans; you need to spread propaganda about plans for reform which are beneficial to the people and which will be implemented once the enemy government is toppled; and you need to convert forces loyal to the enemy and their supporters into ones who are friendly to you. The requirements for psychological warfare in the narrow sense are as follows: you need to fully understand the enemy’s psychological strengths and weaknesses, you need to focus on breaking down enemy commanders psychologically, you need to combine the measures of psychological warfare with operational actions as a means of exerting psychological pressure on the enemy, and you need to strengthen your own psychological training so that you can promptly recognize and avert psychological warfare conducted by the enemy. Commonly used methods of psychological warfare include propaganda, terror, deterrence, deception, confusion, trickery, mollification, and bribery. Dai notes that psychological warfare could be defined as selected information and information media transmitted to listeners (or viewers or readers) in foreign militaries to first influence their feelings, motivation, and objective rational capacity and then to influence the actions of their government, organizations, and groups.

346. What Is Public Opinion Warfare?[\[617\]](#)

Public opinion warfare refers to the use of various mass media by two sides in a conflict to conduct the suppression of information and public opinion in a planned and targeted manner, along with **controlling** international opinion, to create trends in opinion favorable to oneself but unfavorable to the enemy.

Public opinion warfare plays a prominent role in operations conducted under informatized conditions. Public opinion warfare is an important weapon for achieving strategic goals. In the face of the enormous pressure of public opinion, no country or political authority dares to be labeled as the instigator of a war. In order to achieve strategic goals, both sides in a conflict use the news media to transmit planned and incremental strategic news to guide public opinion and gain popular and international support and sympathy. Good reasons for going to war are manufactured, and the war enables the country to achieve its national interests. Regional conflicts since the beginning of the twenty-first century have clearly shown that news and public opinion warfare sit center stage and have become a critical factor in **controlling** how war progresses and indeed determine victory or defeat. Public opinion warfare is an effective means of solidifying a war that emphasizes spiritual domination.

347. What Is Law Warfare?[618]

Law warfare refers to the use of laws as weapons by two sides in a domestic or international conflict, but it refers especially to the laws of war. Multiple means and methods are used to expose the illegality of the enemy's conduct during war and to flaunt one's own conduct as legal.

At the 17th International Symposium on Military Law and War Law, a representative stated that law warfare was a "new weapon" that no other weapon could replace. Whoever masters it will possess the initiative in war. The primary topic in law warfare is war law which includes laws about the use of force, laws about actions in war, laws of neutrality, and laws for punishing war criminals.

According to the Geneva Convention, Dai notes, armed forces need to be accompanied by legal consultants. The ratio of legal consultants in foreign militaries to the total number of personnel in armed forces varies. In the US military it is 1 to 550, while in the Australian military it is 1 to 750. The ranks of legal consultants (lawyers) in foreign militaries are the same as for commanders at the same level, the highest rank being lieutenant general. Civilian staff are ranked as assistant professors. During the Gulf War, the US military sent out more than 2,000 lawyers with the Army. Regardless of whether it was the Gulf War or the wars in Kosovo, Afghanistan or Iraq, law warfare has played an important role in all of these conflicts. Law warfare employs legal **countermeasures** as its primary means of combat.

348. What Is Space Warfare?[619]

Space warfare is composed of the forces of aerospace, and it involves gaining, maintaining, and using superiority in space by conducting a series of operational actions in cosmic space. Space warfare has special forms and methods of operation due to the nature of its operational space and its special weapons systems. Space warfare is divided into different categories: there are space-to-space operations, in which military aerospace weapons engage in combat in outer space; space-to-ground operations, where space weapons platforms utilize attack weapons against targets on the ground; ground-to-space operations, where guided missiles, kinetic energy, and directed energy weapons are used from the ground to strike against aerospace weapons or work stations on the ground which support them; atmospheric space-to-cosmic space operations, where operational aircraft in atmospheric space carry anti-satellite weapons to launch anti-satellite, anti-

spacecraft, and anti-space-platform missiles; and atmospheric space and ground integrated operations, in which aerospace forces play the major role and army, navy, and air forces coordinate closely with them in joint operational actions. In terms of targets, space warfare can be divided into the categories of satellite attacking-and-defending warfare, missile interception and anti-interception warfare, spacecraft and airborne weapons platform attacking-and-defending warfare, space-to-ground attacking-and-defending warfare, ground-to-space attacking-and-defending warfare, and ground-based system destructive warfare. In terms of operational objectives and tasks, space warfare can be divided into forms of operations such as space clampdowns, space attacks, space breakthroughs, space defense, and space information support. Space warfare is the peak of informatized operations. Space is going to become a major battlefield in informatized war. It will be the “commanding height” from which to view military conflicts, and the “high frontier” of national security.

349. What is Chip Warfare?[620]

“Chip warfare” refers to **countermeasures** and combat used in attacking and defending the central processing units (CPUs) in computer subsystems within information systems by two sides in a conflict. At present, this refers to the opponent’s C4ISR systems, weapon strike systems, and logistical support systems which are **controlled** by people, and thus will impact operational actions. Chip warfare is unconventional with no boundaries between military and nonmilitary systems, strategy or tactics, or moral or psychological taboos. The primary way of implementing chip warfare is to preset artificial traps in the military information computer systems of the enemy and interfere with or destroy their operation. There are two types of preset traps: hardware and software traps. Hardware traps primarily refer to “fixing” a virus onto the chip in the central processor of a computer so that when it is installed and used the virus is implanted directly onto the computer, thus destroying the computer system. Some countries are currently developing military viruses which are fixed onto integrated circuit chips and incubate for a long time. They can be activated remotely or when they receive a specified frequency signal. They can also send out a wireless telecommunications signal which identifies their position. According to reports, during the war in Iraq the US military replaced chips so that computer viruses were injected into the anti-air **control** systems of the Iraqi military, the effect of which was to make the war a breeze for the Americans.

Study Guide for Information Operations Theory
400 Questions on Information Operations
Academy of Military Sciences Press
2005

Table of Contents

Editor in Chief: Xu Genchu
Chief Examiner: Dai Qingmin
Publisher: Academy of Military Science Press
Date of Publication: 2005

Executive Editor in Chief: Jiang Lianju

Compiled By: Ye Zheng, Jiang Lianju, Hao Yeli, Jing Jisheng, Lu Zhian, Wang Liwen, Rong Hui, Ji Yubo, Ruan Guangfeng, Yang Yilin, Ling Shan, Li Li, Wang Yonghua, Guo Peng, Zhang Chunyu

Copy Editing By: (Listed by number of strokes in surname) Wang Baocun, Liu Jinsheng, Li Deyi, He Lei, Wu Daiming, Lin Congguang, Cha Jinlu, Hou Xigui, Huang Xing

ISBN 7-80137-911-X, Issued by the Academy of Military Sciences Press (Qinglong Bridge, Haidian District, Beijing 100091), Tel: (010) 6288262

FORWARD	(1)
PART ONE	
INFORMATION AND INFORMATIONIZATION	(1)
(I) INFORMATION	(4)
1. What Is Information?.....	(4)
2. What Are the Basic Elements That Make Up Information?.....	(5)
3. What Are the Relationships Between Matter, Energy, and Information?.....	(6)
4. What Is an Information Society?.....	(6)
5. What Is Information Science?.....	(7)
6. What Are Information Resources?.....	(8)
7. What Are Information Activities?.....	(9)
8. What Are Information Networks?.....	(10)
9. What Is Information Dominance?.....	(10)
10. What Are the Main Characteristics of Information Dominance?..	(11)
11. What Are the Main Criteria for Information Dominance?.....	(12)
12. What Is Information Supremacy?.....	(13)
13. What Is Information Deterrence?.....	(14)
14. What Is an Information Monopoly?.....	(16)
15. How Do We Understand Information Power?.....	(17)
16. What Are Information Borders?.....	(19)
17. What Is a Country's "Information Territory"?.....	(20)
18. What Is "Information Fatigue"?.....	(22)
19. What Is Meant by Striving for Information Dominance, Decision making Dominance, and Action Dominance, and How Have the Three Changed?.....	(23)
20. What Is the Relationship Between Information and Combat?.....	(25)
(II) INFORMATIONIZATION	(26)
21. What Is Informationization?.....	(26)
22. What Is National Informationization?.....	(27)
23. What Is the Idea Behind Informationization?.....	(28)
24. What Is Informationized Military Thought?.....	(29)
25. What is the Relationship Between Informationization and Modernization?.....	(31)
26. What Is the Impact of Informationization on the National Defense Modernization Buildup?.....	(32)
27. How Do We Understand "Disaster Recovery" in the Informationization Buildup?.....	(33)
28. What Are the Material Domain, Information Domain, and Cognition Domain, and How Are They Related?.....	(35)
29. What Is the "Digital Earth"?.....	(35)

30.	What Is the "Information Frontier"?	(37)
31.	What Is the "Theory of Reasonable Sufficiency"?	(37)
32.	What Is the "Theory of Comprehensive Suitability"?	(38)
33.	How Do We Establish a Theory of Informationization with Chinese Military Characteristics?	(39)
34.	How Do We Create Informationized Military Theories?	(40)
35.	What Is the Relationship Between Informationization of the Armed Forces and National Informationization?	(42)
36.	What Is the Relationship Between Informationization of the Armed Forces and Informationized War?	(42)
37.	What Is the Relationship Between Informationization of the Armed Forces and Mechanization of the Armed Forces?	(44)
38.	What Are the Main Differences Between Mechanization and Informationization?	(44)
(III)	THE NEW REVOLUTION IN MILITARY AFFAIRS	(45)
39.	What Is the Relationship Between Informationization of the Armed Forces and the New Revolution in Military Affairs?	(45)
40.	How Did the New Revolution in Military Affairs Arise?	(46)
41.	What Is the Essence of the New Revolution in Military Affairs?	(48)
42.	What Were the Causes that Produced the New Revolution in Military Affairs?	(48)
43.	How Should We Regard the New Revolution in Military Affairs?	(49)
44.	What Are the Main Characteristics of the New Revolution in Military Affairs?	(51)
45.	What Are the Possible Development Trends of the New Revolution in Military Affairs?	(52)
46.	What Are the Main Effects of the New Revolution in Military Affairs on the Buildup of the Armed Forces?	(53)
47.	What Are the Main Effects of the New Revolution in Military on War?	(55)
48.	What Are the Main Effects of the New Revolution in Military on Operation Theories?	(57)
49.	What Are the Main Effects of the New Revolution in Military on Forms of Operations?	(58)
50.	What Are the Main Different Understandings Concerning the World Revolution in Military Affairs?	(60)
51.	How Do We Understand the Revolution of Military Affairs with Chinese Characteristics?	(62)
PART TWO	INFORMATIONIZED OPERATIONS	(65)
(I)	INFORMATION WARFARE, INFORMATIONIZED OPERATIONS, AND INFORMATIONIZED WAR	(68)
52.	What Is Information Warfare?	(68)
53.	What Are Informationized Operations?	(70)
54.	What Are Informationized Operations?	(71)

55.	What Are Operations under Informationized Conditions?.....	(73)
56.	What Is Informationized War?.....	(73)
57.	What Is the Outlook of Informationized War?.....	(74)
58.	What Is Information Security Strategy?.....	(76)
59.	What Are "Non-State Actor" Threats?.....	(78)
60.	What Are Diversified Security Threats?.....	(79)
61.	What Is Information Terrorism?.....	(80)
62.	What Are Information Operations?.....	(81)
63.	What Is Information Space?.....	(82)
64.	What Is Strategic Information Warfare?.....	(82)
65.	What Is Battlefield Information Warfare?.....	(82)
66.	What Do the Contents and Forms of Battlefield Information Warfare Entail?.....	(83)
67.	To What Issues in the Development Trends and the Process of Developing References in Informationized War Should We Pay Attention?.....	(83)
68.	What Are the Main Contents of Plans for Information Operations?.....	(84)
69.	What Is Information Offense?.....	(85)
70.	What Are the Basic Requirements of Operations for Capturing Information Supremacy?.....	(87)
71.	What Is Information Defense?.....	(88)
72.	What Is Information Security?.....	(90)
73.	What Is Network Psychological Warfare?.....	(91)
74.	What Is Intelligence Warfare?.....	(91)
75.	What Is Precision Warfare?.....	(92)
76.	What Is Electronic Warfare?.....	(93)
77.	What Is Electronic Surveillance?.....	(94)
78.	What Is Electronic Offense?.....	(95)
79.	What Is Electronic Defense?.....	(96)
80.	What Is Computer Network Warfare?.....	(96)
81.	What Is Command and Control Warfare?.....	(97)
82.	What Is Structural Destruction Warfare?.....	(98)
83.	What Is Hard Destruction?.....	(100)
84.	What Are Soft Kills?.....	(100)
85.	What Is Integrated Electronic and Network Warfare?.....	(100)
86.	What Is Virtual Warfare?.....	(101)
87.	What Is Navigation Warfare?.....	(101)
88.	What Is Military Deception?.....	(102)
(II)	PRODUCING AND DEVELOPING INFORMATIONIZED OPERATIONS.....	(103)
89.	What Are the Stages of Development of Informationized Operations?.....	(103)
90.	Why Do We Say That the Gulf War Was the Embryonic Form of Informationized War?.....	(105)
91.	From the Stance of Informationization, What New	

	Characteristics Did the Kosovo War Have?.....	(106)
92.	What Aspects of the Afghanistan War Demonstrated the Characteristics of Informationized War?.....	(108)
93.	Why Was the Iraq War a Typical Informationized War?.....	(109)
(III)	THE CHARACTERISTICS, RULES, AND PRINCIPLES OF INFORMATIONIZED WAR.....	(111)
94.	What Are the Characteristics of Informationized Operations?...	(111)
95.	What Are the Rules of Informationized Operations?.....	(113)
96.	What Are the Main Features of Informationized Operations?....	(115)
97.	What Are the Principles of Informationized Operations?.....	(117)
98.	What Are the New Changes in Informationized Operations?....	(119)
99.	What Systems Support Informationized Operations?.....	(121)
100.	What Are the Basic Contents of the "Dual Historic Tasks" of Mechanization and Informationization?.....	(122)
101.	What Are the Differences Between Informationized Operations and Mechanized Operations?.....	(124)
102.	What Is the Relationship Between Informationized Operations And Mechanized Operations?.....	(126)
103.	What Are the New Characteristics of Offensive Operations Under Informationized Conditions?.....	(127)
104.	What Are the New Characteristics of Defensive Operations Under Informationized Conditions?.....	(130)
105.	What Are the New Characteristics of Battlefield Mobility Under Informationized Conditions?.....	(131)
106.	How Is the Joint Integrated Operations System Constructed and How Does It Operate?.....	(133)
PART THREE	INFORMATION TECHNOLOGY.....	(137)
(140)	107. What Is Information Technology?.....	
(140)	108. What Is Artificial Intelligence?.....	
(141)	109. What Is the Military Expert System?.....	
(142)	110. What Is Model Building Technology?.....	
(143)	111. What Is Simulation Technology?.....	
	112. What Are Information Countermeasure Technologies?.....	(145)
	113. What Are Non-Information System Counter-Detection Technologies?.....	(146)
	114. What Are Information Jamming Technologies?.....	(147)
	115. What Are Information Anti-Jamming Technologies?.....	(150)
	116. What Are Information System Destruction Technologies?.....	(152)
	117. What Are Information System Counter-Destruction Technologies?.....	(153)
	118. What Are Comprehensive Integration Technologies?.....	(154)

	119.	What Are Optimization Technologies?.....	(156)
(157)	120.	What Are Computer Viruses?.....	
(159)	121.	What Are Information Concealment Technologies?.....	
	122.	What Are Information Prototype Technologies?.....	(160)
	123.	What Are Anti-Information Strategy Technologies?.....	(161)
(162)	124.	What Are Radio Frequency Identification Technologies?.....	
	125.	What Are the Identification Friend or Foe Technologies on the Informationized Battlefield?.....	(163)
	126.	What Are the High and New Technologies in Intelligence Reconnaissance?.....	(164)
	127.	What Are the High and New Technologies in Early Warning Detection?.....	(168)
	128.	What Are the Main High and New Technologies in Detecting and Stealing Information?.....	(170)
	129.	What Are the Principles for the Functions of Information Warfare?.....	(171)
	130.	What Are the Five Kinds of Technology in Non-Contact Operations?.....	(173)
	131.	What Are the Main Technologies for Information Security Assurance in China's Armed Forces?.....	(173)
	132.	What Main Energy and Power Technologies Does the Military Currently Have?.....	(173)
	133.	What Is Military Opto-Electronic Technology?.....	(174)
	134.	What Are new Military Material Technologies?.....	(175)
	135.	How Do We Fully Bring into Play the Role of Information Technology in the Informationization Buildup of the Armed Forces?.....	(175)
	136.	What Are the Detection Technologies for the Maritime Battlefield Environment?.....	(176)
	137.	What Geographical Environment Information Acquisition Technologies Exist for Littoral Space?.....	(178)
PART FOUR		INFORMATIONIZED FORCES.....	
(181)	(I)	INFORMATIONIZED ARMED FORCES.....	(184)
	138.	What Is an Informationized Armed Force?.....	(184)
	139.	What Are the Main Characteristics of an Informationized Armed Force?.....	(184)
	140.	What Are Digitized Units?.....	(185)
	141.	What Are Electronic Warfare Units?.....	(186)
	142.	What Are Network Warfare Units?.....	(186)
	143.	What Are Rapid Reaction Units?.....	(187)
	144.	What Are "Hackers"?.....	(188)
	145.	What Are "Informationized Troops"?.....	(189)

146.	What Is an "All-Round Armed Force"?	(191)
147.	What Are Traditional Forces, Transitional Forces, and Objective Forces?	(191)
148.	What Are "Modular" Units?	(192)
149.	What Is an Expeditionary Air and Space Force?	(193)
150.	What Is an Informationized Global Engagement Task Force?..	(195)
151.	What Is an Information Warfare Aviation Force?	(195)
152.	What Are the "Trends in the Informationization of Military Strategy"?	(195)
153.	What Is the "Strategy for Information Dominance"?	(196)
154.	What Is the "Strategy for Information Warfare"?	(197)
(II)	INFORMATIONIZATION OF THE ARMED FORCES.....	(199)
155.	What Is Informationization of the Armed Forces?	(199)
156.	What Are the Main Features of Informationization of the Armed Forces?	(201)
157.	What Are the Main Characteristics of the Informationization Of China's Military?	(202)
158.	What Is Promoting the Key Elements of the Informationization of China's Military?	(203)
159.	What Are the Main Contents Included in the Informationization of the Armed Forces?	(204)
160.	How Do We Make Full Use of Civilian Information Resources to Raise the Informationization Level of China's Military?	.
(205)		
161.	What Are the Basic Elements of the Informationization Buildup of China's Military?	(206)
162.	What Are the Relationships Among the Informationization Buildup, High Technology War, and Informationized War?....	(207)
163.	What Relationship Does the Informationization Buildup of the Armed Forces Have with Other Buildups?	(208)
164.	How Do We Understand the System of Regulations and Standards That Must Be Perfected in Promoting the Informationization Buildup of China's Military?	(209)
165.	What Is Top-Down Design?	(210)
166.	How Do We Properly Make a Top-Down Design in the Informationization of China's Military?	(211)
167.	How Do We Establish a Scientific and Highly Effective System for Guiding the Informationization Buildup?	(213)
168.	What Is Our Understanding of the Need to Adhere to a Coordinated Development Strategy for Informationization of the Armed Forces and National Informationization?	(214)
169.	What Is Our Understanding of How the Informationization Buildup Should Be Centered on Command and Control Systems?	(214)
170.	What Are the Main Principles of the Information Security	

	Buildup?.....	(215)
PART FIVE	INFORMATIONIZED WEAPONRY.....	(219)
	INFORMATIONIZATION OF WEAPONRY.....	(222)
(I)	171. What Is Informationized Weaponry?.....	(222)
	172. What Is Informationization of Weaponry?.....	(223)
	173. What Are Informationized Ammunitions?.....	
(223)		
	174. What Are Informationized Operations Platforms?.....	
(224)		
	175. What Are Informationized Single Soldier Weapons Systems?...	
(225)		
	176. What Are the Main Features of the Use of Weapons Systems in Informationized War?.....	(227)
	177. What Are the Relationships That Building Informationized Weapons Systems Should Handle Well?.....	(227)
	178. What Is the "Theory of Critical Mass"?.....	
(229)		
	179. What Is "Embedding" Informationization?.....	
(230)		
	180. What Are the Development Trends in Weaponry Integration?....	
(230)		
	181. Where Should the Focus Be Placed in Accelerating the Buildup Of Informationized Weapons?.....	(231)
	182. How Do We Control the Relationship Between the Buildup of Weaponry Informationization and the Mechanization Buildup?..	(232)
	(II) INFORMATIONIZED WEAPONS.....	(234)
	183. What Are Informationized Weapons?.....	
(234)		
	184. What Are Stealth Weapons?.....	
(234)		
	185. What Are Intelligent Anti-Helicopter Mines?.....	
(235)		
	186. What Are Electromagnetic Pulse Bombs?.....	
(236)		
	187. What Are Graphite Bombs?.....	
(237)		
	188. What Are Offensive Computer Network Weapons?.....	
(238)		
	189. What Are Defensive Computer Network Weapons?.....	
(238)		
	190. What Are Computer Virus Weapons?.....	
(239)		
	191. What Are "Trojan Horse" Programs?.....	
(240)		
	192. What Are Logic Bombs?.....	
(240)		

(241)	193.	What Are Computer "Traps"?	
(241)	194.	What Are Micrometer/Nanometer Robots?	
(242)	195.	What Are High Energy Radio Frequency Guns?	
(242)	196.	What Are Knowbots?	
(243)	197.	What Are Robot Soldiers?	
(244)	198.	What Are Chip Bacteria?	
(244)	199.	What Are Power Destruction Bombs?	
(245)	(III)	NEW CONCEPT WEAPONS	
(245)	200.	What Are New Concept Weapons?	
(245)	201.	What Are the Main Characteristics of New Concept Weapons?...	
(246)	202.	What Are Directed Energy Weapons?	
(246)	203.	What Are Laser Weapons?	
(248)	204.	What Are High Power Microwave Weapons?	
(249)	205.	What Are Electromagnetic Weapons?	
(249)	206.	What Are Ion Weapons?	
(250)	207.	What Are Genetic Weapons?	
(251)	208.	What Are New Materials Weapons?	
	209.	What Are High Temperature/High Pressure/Cold Temperature Weapons?	(252)
(252)	210.	What Are Lightning and Solar Weapons?	
(252)	211.	What Are Fog Weapons?	
(253)	212.	What Are Artificial Environment Weapons?	
(253)	213.	What Are Oxygen Absorbing Weapons?	
(254)	214.	What Are Particle Beam Weapons?	

(255)	215.	What Are Kinetic Energy Weapons?.....	
(255)	216.	What Are Non-Lethal Weapons?.....	
(256)	217.	What Are Subsonic Wave Weapons?.....	
(257)	218.	What Are New Concept Explosives?.....	
(258)	219.	What Are Space Planes?.....	
(259)	220.	How Are Space Weapons Categorized?.....	
	PART SIX	INFORMATIONIZED BATTLEFIELD ENVIRONMENT....	(263)
	(I)	THE INFORMATIONIZED BATTLEFIELD.....	(266)
(266)	221.	What Is the Informationized Battlefield?.....	
(266)	222.	What Is the Digitized Battlefield?.....	
(267)	223.	What Is the Battlefield Information Environment?.....	
(267)	224.	What Characteristics Does the Informationized Battlefield Have?..	
(269)	225.	What Are the Characteristics of the Battlefield Information Environment?.....	(268)
(270)	226.	What Effect Does the Atmospheric Environment Have on War?.....	
	227.	What Is the Maritime Battlefield Environment?.....	
	228.	What Are the Main Characteristics of Building Up the Maritime Battle Environment?.....	(272)
(272)	229.	What Effect Does the Physical Maritime Environment Have on Military Activities?.....	
(276)	230.	What Is the Space Battlefield?.....	
(276)	231.	What Is Outer Space?.....	
(277)	232.	What Is Space Supremacy?.....	
(278)	233.	What Is Air Supremacy?.....	
(279)	234.	What Is Electromagnetic Supremacy?.....	
(280)	235.	What Is Rapid Dominance?.....	
	236.	How Are the Orbits of Space Vehicles Categorized?.....	

(281)	237.	What Huge Benefits Does Outer Space Include?.....	
(282)	238.	What Is the Distributed Virtual Battlefield Environment?.....	
(284)	239.	What Is the All-Inclusive War Drilling Field?.....	
(285)	(II)	BATTLEFIELD INFORMATION SYSTEMS.....	
(286)	240.	What Are Information Systems?.....	
(286)	241.	What Are the Basic Architecture and Functions of Information Systems?.....	
(286)	242.	What Are Military Electronic Information Systems?.....	
(286)	243.	What Are the Basic Functions of Military Electronic Information Systems?.....	(287)
	244.	What Are the Categories of Military Electronic Information Systems?.....	(287)
	245.	What Are the Development Trends for Military Electronic Information Systems?.....	(288)
	246.	What Are the Security Assurance Systems for Military Information Systems?.....	(289)
(290)	247.	What Are Command and Control Systems?.....	
(290)	248.	What Are Information Retrieval Systems?.....	
(291)	249.	What Are Communications Systems?.....	
(291)	250.	What Are Electronic Countermeasures Systems?.....	
(291)	251.	What Are Navigational Systems?.....	
(292)	252.	What Are Space Surveillance Systems?.....	
(292)	253.	What Are Comprehensive Assurance Systems?.....	
(293)	254.	What Are Space Vehicle Launch Sites?.....	
(294)	255.	What Are Space Monitoring Networks?.....	
(294)	256.	What Is C ⁴ IKSR?.....	
(295)	257.	What Is MIDS?.....	

(295)	258.	What Are Data Links?.....	
	259.	What Are the Main Developments in the Data Links of Foreign Militaries?.....	(296)
(298)	260.	What Is the "Global Information Grid"?.....	
(301)	261.	What Is FBCB2.....	
(301)	262.	What Is GPS.....	
(302)	263.	What Is a Geospatial Database?.....	
(303)	264.	What Is a Digital Elevation Database?.....	
(305)	265.	What Is a Multiple Resolution Orthophoto Database?.....	
(305)	266.	What Is a Basic Features Database?.....	
(306)	267.	What Is a Target Positioning Database?.....	
	PART SEVEN	INFORMATIONIZED OPERATIONS COMMAND...	(309)
(312)	268.	What Is Informationized Operations Command?.....	
	269.	What Are the New Characteristics of Informationized Operations Command?.....	(312)
	270.	What Are the New Changes in a Comparison of Operational Command under Informationized Conditions and Traditional Operational Command?.....	(314)
	271.	What Are the Development Trends in Operational Command under Informationized Conditions?.....	(316)
	272.	What Are the Basic Demands of Informationized Operations on Organizational Command?.....	(317)
	273.	What Elements Should Be Controlled to Improve Command Effectiveness Under Informationized Conditions?.....	(318)
	274.	How Do We Create a Command System That Is Suited to Operations under Informationized Conditions?.....	(320)
	275.	What Demands Do Informationized Operations Impose on Building Command Systems?.....	(321)
	276.	What Are the New Features of the Revolution in Command Methods Under Informationization Conditions?.....	(322)
	277.	How Do We Fortify Command Information Systems under Informationized Conditions?.....	(323)
	278.	What Kinds of Ideas for Operational Command are Brought About under Informationized Conditions?.....	(324)
	279.	How Is a High Degree of Intelligence Sharing Brought About Under Informationized Conditions?.....	

(325)	280.	What New Changes Are There in Command Communications in Informationized Operations?.....	(326)
	281.	What New Developments Are There in Military Mapping in Informationized Operations?.....	(326)
	282.	What Is the Main Role of Remote Sensing Imaging in Informationized Operations?.....	(328)
	283.	What Are Global Command Systems?.....	
(330)	284.	What Are Imaging and Geospatial Information Service Systems?....	
(330)	285.	What Is the Visualization of Scientific Calculations?.....	
(331)	286.	What Is the Visualization of the Battlefield?.....	
(332)	287.	What Is the Main Substance of the Visualization Products for the Digitized Battlefield?.....	
(332)	288.	What Is Simulation of Battlefield Environments?.....	
(333)	289.	What Are the Main Uses for Electronic Maps?.....	
(334)	290.	What Are Pocket-Sized Electronic Map Systems?.....	
(335)	291.	What Are General Operational Maps?.....	
(336)	292.	What Are New Concept Military Maps?.....	
(339)		PART EIGHT INFORMATIONIZED OPERATIONAL SUPPORT....	(339)
	(I)	INFORMATIONIZED OPERATIONAL LOGISTICS AND EQUIPMENT SUPPORT.....	(342)
(342)	293.	What Is Informationized Support?.....	
(342)	294.	What Are Focused Logistics?.....	
(343)	295.	What Are Visual Logistics?.....	
(344)	296.	What Is Immediate Logistical Supply?.....	
(344)	297.	What Is the "Revolution in Military Logistics"?.....	
(345)	298.	What Is the Impact of Informationization on Logistical Support.....	
(346)	299.	How Do We Improve Informationized Logistical Support Capabilities?.....	

(347)	300.	What Are the Characteristics of Goods and Materials Support for Informationized Operations?.....	
(347)	301.	What Are the New Measures for Goods and Materials Support for Informationized Operations?.....	
(349)	302.	What Is the Impact of Informationized Operations on Medical Services Support?.....	
(350)	303.	What Are the Impact and Demands of Informationized Operations On Equipment Support?.....	
	304.	What Are the New Changes in Equipment Support in Informationized Operations?.....	(352)
	305.	What Are the Main Characteristics of Equipment and Technology Support in Informationized Operations?.....	(352)
	(II)	OPERATIONAL INFORMATION SECURITY ASSURANCE..	(353)
(353)	306.	What Is Operational Information Security Assurance?.....	
(354)	307.	What Are Network Sentries?.....	
(354)	308.	What Are Information Defense Encryption Systems?.....	
(354)	309.	What Is a Firewall?.....	
(355)	310.	What Are Multi-Layered Network Defense Systems?.....	
(355)	311.	What Is Operational Secrecy?.....	
(356)	312.	What Are the Main Threats Facing Information Security?.....	
	313.	What Are the Main Tasks of Operational Information Security Assurance?.....	(367)
	314.	What Are the New Issues Confronting Operational Information Security Assurance?.....	(368)
	315.	What Are the New Situations and New Issues Presently Confronting the Information Security Assurance of China's Military?.....	(369)
	316.	What Matters Should Be Attended To and Resolution in Enhancing Operational Information Security Assurance?.....	(370)
	317.	What Is the Status of Information Security in Informationized Operations?.....	(371)
	318.	What Are the Main Threats Confronting the Security of Information Systems?.....	(372)
	319.	What Are the New Characteristics of Defending the Security of Information Systems?.....	(373)

	320.	What Technical Measures Are There for Assuring the Security of Information Networks?.....	(374)
(374)	321.	How Do We Enhance Information Network Security?.....	
	322.	What Are the Development Trends for Defending the Security of Information Systems?.....	(375)
PART NINE		FORMS OF INFORMATIONIZED OPERATIONS.....	
(377)	(I)	JOINT OPERATIONS.....	
(380)	323.	What Are the Concepts and Characteristics of Integrated Joint Operations?.....	(380)
	324.	What Are the Major Changes When Informationized War Is Compared to Mechanized War?.....	(380)
	325.	What Are the New Characteristics and Contents of Joint Firepower Engagement Operations Under Informationized Conditions?.....	(384)
	326.	What Are the New Characteristics and Contents of Offensive Island Operations Under Informationized Conditions?.....	(384)
	327.	What Are the New Characteristics and Contents of Island Blockade Operations under Informationized Conditions?.....	(385)
	328.	What Are the New Characteristics and Contents of Anti-Landing Operations under Informationized Conditions?.....	(387)
(388)	329.	What Are the New Characteristics and Contents of Counterattack Operations under Informationized Conditions in Border Areas?.....	
	330.	What Are the New Characteristics and Contents of Anti-Air Attack Operations under Informationized Conditions?.....	(389)
	331.	What Are the Main Changes in Air Defense Operations under Informationized Conditions?.....	(390)
	332.	What Are the New Changes in Information Operations under Informationized Conditions?.....	(392)
	333.	What Are the New Characteristics of Special Operations under Informationized Conditions?.....	(393)
	334.	What Are the Main Characteristics of Anti-Terrorism Operations under Informationized Conditions?.....	(394)
(395)	335.	What Is System Sabotage Warfare?.....	
(396)	336.	What Is Network Centric Warfare?.....	
(399)	337.	What Are Non-Contact Operations?.....	
(400)	338.	What Are Non-Linear Operations?.....	
(400)	339.	What Are Asymmetric Operations?.....	
	340.	What Is "Operations Centric Warfare"?.....	

(401)	341.	What Are "Omni-Directional High Level Operations"?	
(402)	342.	What Are "Full Spectrum Operations"?	
(402)	343.	What Are "Stable Operations"?	
(403)	344.	What Is "Three Warfare"?	
(403)	345.	What Is Psychological Warfare?	
(404)	346.	What Is Public Opinion Warfare?	
(405)	347.	What Is Law Warfare?	
(406)	348.	What Is Space Warfare?	
(407)	349.	What Is "Chip Warfare"?	
(408)	(II)	INFORMATIONIZED OPERATIONS OF THE MILITARY BRANCHES	
			(409)
	350.	What Are the Characteristics of the Informationized Operations of the Army?	(409)
	351.	What Are the Features That Are Displayed on the Informationized Ground Battlefield?	(410)
	352.	In What Ways Are the Status and Role of Army Reflected in Informationized Operations?	(413)
	353.	What Are the Characteristics of the Informationized Operations of The Navy?	(413)
	354.	What Are the Features That Are Displayed on the Informationized Sea Battlefield?	(414)
	355.	In What Ways Are the Status and Role of the Navy Reflected in Informationized Operations?	(415)
	356.	What Are the Full Dimensional Detection Measures for Submarines in the 21st Century?	(416)
	357.	What Are the Characteristics of the Informationized Operations of the Air Force?	(417)
	358.	What Are the Features That Are Displayed on the Informationized Air Battlefield?	(418)
	359.	In What Ways Are the Status and Role of the Air Force Reflected In Informationized Operations?	(419)
PART TEN		THE MILITARY INFORMATIONIZATION BUILDUPS AND DEVELOPMENTS IN SOME COUNTRIES	(421)
	(I)	THE STATE OF DEVELOPMENT OF THE US MILITARY'S INFORMATIONIZATION	(424)
	360.	What Is the US Military's "Joint Vision 2010"?	

(424)	361.	What Is the US Military's "Joint Vision 2020"?.....	
(426)	362.	What Is the State of Development of the US Military's Operational Theories for Informationization?.....	(429)
	363.	What is the State of Development of the US Military's Information Systems?.....	(431)
	364.	What is the State of Development of the US Military's Informationized Weaponry?.....	(434)
	365.	What is the State of Development of the US Military's Informationized Force?.....	(436)
	366.	What is the State of the Building of the US Military's Informationized Battlefield?.....	(438)
	367.	What Is the State of the US Military's Informationization Training?.....	(439)
	368.	What is the State of the Adjustments to the US Military's Organizational Structure?.....	(440)
	369.	What Are the Development Trends of the Informationization of The US Military?.....	(441)
	370.	What Is the Goal of the US Army's Informationization Development?.....	(442)
	371.	What Is the Goal of the US Navy's Informationization Development?.....	(443)
	372.	What Is the Goal of the US Air Force's Informationization Development?.....	(443)
	373.	In the End, Is the US Strategic Missile Defense System Useful?....	
(445)	374.	What Space Surveillance Forces Does the US Have?.....	
(446)	375.	What Is the Current Status of US Electronic Reconnaissance Satellites?.....	(448)
	376.	How Is the Buildup of the US Military's Future "Net Force"?.....	
(449)	377.	What Is the State of Development of US Early Warning Satellites?	
(452)	(II)	THE STATE OF DEVELOPMENT OF THE RUSSIAN MILITARY'S INFORMATIONIZATION.....	(453)
	378.	What Is the State of Development of the Russian Military's Theories on Informationized Operations?.....	(453)
	379.	What Is the State of Development of the Russian Military's Informationized Weaponry?.....	(454)
	380.	What Is the State of Development of the Russian Military's Information Systems?.....	(455)
	381.	What Is the State of the Adjustments to the Russian Military's Organizational Structure?.....	(456)
	382.	What Are the Development Trends of the Information Systems of	

	the Russian Military?.....	(456)
383.	What Are the Development Trends of the Informationized Weaponry of the Russian Military?.....	(457)
384.	What Is the State of Development of Russia's Early Warning Satellites?.....	(457)
(III)	THE STATE OF DEVELOPMENT OF THE JAPANESE MILITARY'S INFORMATIONIZATION.....	(459)
385.	What Is the State of Development of the Japanese Military's Theories on Informationized Operations?.....	(459)
386.	What Is the State of the Buildup of the Informationized Force of the Japanese Military?.....	(460)
387.	What Is the State of the Buildup of the Information Systems of the Japanese Military?.....	(461)
388.	What Is the State of Development of Informationized Weaponry of the Japanese Military?.....	(463)
389.	What Are the Development Trends of the Information Systems of the Japanese Military?.....	(465)
390.	What Are the Development Trends of the Informationized Weaponry of the Japanese Military?.....	(465)
391.	What Are the Development Trends of the Informationized Operational Capabilities of the Japanese Military?.....	(466)
(IV)	THE STATE OF DEVELOPMENT OF THE INDIAN MILITARY'S INFORMATIONIZATION.....	(466)
392.	What Is the State of Development of the Indian Military's Theories on Informationized Operations?.....	(466)
393.	What Is the State of Development of the Informationized Weaponry of the Indian Military?.....	(467)
394.	What Is the State of the Building of the Indian Military's Information Systems?.....	(469)
395.	What Is the State of the Indian Military's Preparations for Informationized Operations?.....	(470)
396.	What Is the State of the Indian Military's Development and Making Use of Information Resources?.....	(470)
397.	What Are the Development Trends of the Informationization of the Indian Military?.....	(471)
398.	What Are the Development Trends of the Indian Military's Information Systems?.....	(472)
399.	What Are the Informationization Development Trends of the Indian Military's Weaponry?.....	(472)
400.	What Is the State of India's Development of a New Missile Defense System?.....	(473)
	MAIN REFERENCES AND MATERIALS.....	(474)

CHAPTER NINE: WARFARE STRATEGY THEORY

This chapter focuses on informationization topics discussed in Warfare Strategy Theory, 2005. [621]

Introduction

The discussion in this chapter ends Decoding the Virtual Dragon in much the way it began—with a look at IW/IO through the eyes of Major General Yao Youzhi. Yao served as a co-editor of the book reviewed in Chapter One (The Science of Military Strategy) and as the Editor-in-Chief of this chapter's focus, Warfare Strategy Theory. This provides an opportunity for the reader to compare Yao's information warfare analysis in 2001 with this 2005 work.

The 2001 book had only one chapter on informationization and that chapter focused on strategic IW. The 2005 book specifically highlights the informationization topic in seven of the book's 37 chapters. In that respect Yao has expanded his informationization focus. In addition, the latter work provides an expanded look at the features of war in the twenty-first century. These include examinations of the Chinese definition and discussion of asymmetric, nontraditional, antiterror, and nuclear warfare concepts among others. The asymmetric discussion is included in this chapter due to its relevancy to informationization forces. For example, Yao noted that network centric war uses information technology to gain an asymmetric information advantage. [622]

Yao's new work has four sections: warfare concepts, features of war, war preparations, and implementation. He and his co-editors use US Gulf War and Iraq War experiences for emphasis whenever possible. The Table of Contents is located at the end of the chapter.

Informationized Warfare

Yao devotes an entire chapter in Warfare Strategy Theory specifically to informationized warfare. Here Yao defines informationized war as warfare conducted with both sides engaged in war mainly using informationized weapons and the methods of operations that go along with it. He believes it is possible for informationized warfare to be waged by just one side in a conflict. Information-age warfare is a broader concept that represents the integration of various kinds of warfare. [623]

Yao notes that the first person in China to use the term "informationized warfare under conditions of nuclear deterrence" was scientist Qian Xuesen in 1995. Before long this term was widely used in China. Thus while Shen is noted as the father of information warfare in China (writing first in 1985), Qian is seen by Yao as the developer of the informationized warfare under nuclear deterrence concept. [624]

Informationized warfare has four main elements:

- An informationized weaponry system that includes three systems: an informationized

weapons system, an informationized sensor system, and an informationized command and control system

- An informationized operations theory that includes warfare supremacy theories, new operational principles (attacking a center of gravity, decapitation, simultaneous operations, full-spectrum dominance, etc.), and new combat theories and forms of combat (asymmetry, noncontact and nonlinear operations, network-centric warfare, and so on)
- An informationized military organizational structure that gives prominence to: flattened and networked systems; downsizing and modularizing the force structure; increasing the proportion of the navy, air force and strategic missile force; building an integrated joint force with all branches and services; and developing new branches and services (such as IW, network warfare, and space warfare)
- And personnel suited to informationized warfare.[\[625\]](#)

In addition to these concepts, informationized warfare exhibits new characteristics that include transparency, real-time attacks, precision, and effective use of force. Transparency allows the battlefield to become clearer for friendly forces while providing opportunities to increase an opponent's "fog of war" via information overload. This also means trapping the enemy in the fog of war through the degradation of his information collection source, through the monopolization of high-technology information resources, and through the establishment of information traps.

Chinese estimates are that during the Iraq War of 2003 the US knew more than 90% of the significant events on the battlefield through the use of sensors. The battlefield sensor system included space, airborne, and ground/sea sensors capable of integrating their findings and creating a multilayered omnidirectional deployment system.[\[626\]](#) This allowed the US to increase the enemy's fog of war through the methods described.

Sensor technologies help a force to stay current to the rapidly changing information situation around them and conduct real-time attacks. These attacks include obtaining information, making decisions, taking action, and completing attacks in the immediate future. The lifespan of information has grown shorter and battlefield awareness must be constantly updated. The Chinese believe that the cycle of discovering targets and attacking them changed from twenty-four hours in the Gulf War to two hours in Kosovo to ten minutes in the Iraq War. This quick response mechanism has been aided by a highly developed C4ISR system and a developed global information grid (GIG) in the US.[\[627\]](#)

Informationized weapons are precise and controllable, and they are practically unaffected by clouds, mist, dust, or thick smoke. Precision target, firepower, and attack intensity control are the main precision operations. Due to precision operations, the use of force and the function of information power is now more effective in terms of killing power, integration power, and psychological attack power than ever before. Previous psychological effects that could only be attained with mass destruction can now be attained using informationized conventional weapons. According to Yao the US military can track victims or uncover their whereabouts at a moment's notice and this places tremendous psychological pressure on an enemy force. Precision-guided munitions can quickly attack and catch combatants completely unaware. Psychological warfare has transformed into a form of strategic operation and has moved into politics, economics, diplomacy,

and culture.[\[628\]](#)

Informationization integrates man and machine to an extent never before possible and the US has capitalized on this point to enable the rapid development of countermeasures and counterstrategies. A new phase of integrated-information countermeasures and firepower destruction has also arisen. The Chinese note that the US did not relax its countermeasure research in the areas of knowledge, intelligence, and strategy because it possessed advanced weapons.[\[629\]](#)

Informationized weapons are also forcing the further integration of the armed forces and the masses, leading theorists to proclaim that “information warfare is, to a certain degree, another form of ‘People’s War.’”[\[630\]](#) Now there are even higher demands for personnel with science and technology skills to support and participate in informationized war. This also means that informationization can open new territory for unconventional operations and make the latter more powerful. It has already made it easier for guerilla groups to recruit and organize personnel and to command activities.

Noncontact operations will be the most typical form of operations in the era of informationized warfare. This mainly occurs in space, air, and on sea but not as often on the ground in the Chinese opinion since network warfare, electronic warfare, air and missile attacks, and counterattacks are the most prevalent form of noncontact operations. Informationization’s most notable impact on future war is its ability to make informationized weapons such as these into combat force multipliers.

Yao discusses the organic integration of soft and hard kills. New forms of electronic-information countermeasures are attracting attention such as navigation warfare, which focuses on navigational and guidance information. Developing the ability to jam the US military’s cruise missiles is one such issue. Attacking networks is another form of informationized warfare. Networks are usually the softest spot in operational systems according to Yao.[\[631\]](#)

Yao goes on to describe in more detail the form of network-centric warfare. He notes that it will take place in the physical, information, and cognitive domains. The physical domain is the tangible arena of real existence where platforms exist. The information domain is where the real and false are mixed together and where the fight for information dominance and supremacy is conducted. The cognitive domain refers to the mental space of operational personnel. Here is where ideas, awareness, psychology, perception, understanding, emotions, sense of values, and other mental activities exist. The network-centric architecture is made up of sensor systems, information systems (communication satellites, etc.), and a processing system. Network-centric architecture allows, according to Yao, for “decentralized concentration.” In stovepipes of the past, the sum of a force’s combat strength was calculated by adding together all of its parts. Today, the sum of a force’s combat strength is the product of all operational elements, where combat strength conforms to the principle of multiplication: it is the rule of exponential multiplication.[\[632\]](#)

In the opinion of the author of Decoding the Virtual Dragon it is difficult to see how informationized war differs from information war. Perhaps the distinction is reflective of a turf battle in the PLA for information terminology rights. As was evident, most of the points covered

above were accounted for in earlier discussions of IW.

Associated Informationized Aspects of Warfare Strategy Theory

In addition to the separate chapter on informationized warfare discussed above, there are specific sections of other chapters that address the topic of informationization. These sections are

- Reconceptualization of Warfare Objectives under Informationized Conditions
- Features of Informationized Warfare
- The Scale of High Technology Partial War Is Becoming Increasingly Controllable
- New Time and Space Characteristics of Informationized Warfare
- Fully Revised War Concepts Must Be Implemented for Warfare Thought in the Information Age
- Basic Transformations in the Method of Thinking Must Be Implemented for Warfare Thought in the Information Age.

Yao writes that informationized warfare has changed the traditional significance of attack, capture, control, and defend. This is because precision attacks have made possible the destruction of the enemy's entire war system. The primary attack target has become the strategic information system of an enemy force. All activities now revolve around gaining battlefield supremacy whose foundation is information supremacy. Direct destruction of an enemy's will has supplanted total annihilation of an enemy force's military capability. This will invite completely new methods of warfare in future wars.[\[633\]](#)

With regard to features of informationized warfare, Yao lists its main features as follows:

- Informationized weapons are the dominant weapons on the battlefield in the form of platforms and ammunition.
- Information energy (reconnaissance, precision guidance, electronic warfare, etc.) is the principal capability unleashed on the battlefield in that it can control substance and capability.
- Informationized warfare is the principal form of war
- The principle objectives of informationized war are the three major systems of battlefield cognition (surveillance, survey, navigation, etc.), battlefield communication (transmission of information), and battlefield guidance and control.
- Information superiority is the pinnacle of the battlefield struggle. Through information superiority other levels of dominance (airpower, naval space) are then possible.[\[634\]](#)

Yao also notes that since the objectives of a high-tech war are generally limited and total victory (annihilation of the enemy, occupation of the entire territory of the enemy, etc.) is not required, it is important to control the scale of a high-tech war. War control is closely related to the efficiency of the use of the means of war. Instead of taking out troops, the focus becomes attacking nodal points and taking out systems.[\[635\]](#) As a result

Vying for information superiority takes precedence over air superiority and naval superiority, precision attacks are better than city sieges and blanket attacks, destruction of the opposition's will to resist is superior to complete annihilation of the enemy's combat capability, and noncontact war is more powerful than major combat.[\[636\]](#)

With regard to time and space, Yao notes that time is more important due to the speed of transactions. Operations and tempo are accelerated and the combat process is greatly shortened. Now platforms and personnel are integrated and observation tools have broken through prior limitations (night vision, etc.) such that war is becoming all-weather and all-time. Traditional warfare's sequential steps are being modified/disrupted. For example, the US strives for rapid decisive combat and not a slow pace, phase by phase approach. With information transmitted at the speed of light beams, battlefield awareness and decision making have changed. Decisions are made quickly as situations are updated in near real-time. Prewar preparations and the adoption of specific strategies and tactics must take time and space into account if they are to remain effective.[\[637\]](#) Time must be compressed by decreasing the number of links and increasing the information transmission speed.[\[638\]](#)

Another time and space factor is that with the military occupation of intangible (virtual) space, vying for cognitive space has increased in importance as an informationized trend. Cognitive space must be treated as an independent space since the occupation of natural geographical space is moving to an occupation of information and cognitive space.[\[639\]](#) He states that

The war objective of informationized war is manifested even more apparently as forcing the enemy to succumb and accept control rather than the traditional war objectives of taking cities, seizing territories, and directly taking possession of resources. It should be understood that the ultimate objective of war is to take possession of the enemy's cognitive space. Cognitive space is based on the military theory of cognition of combat outcome...the struggle for cognitive space is the highest level of informationized warfare and the objective of the strategic mind war of modern warfare.[\[640\]](#)

Yao also writes that the development of informationized forces must be closely followed so that the PLA can stay abreast of changes in the nature and orientation of warfare. There are ten renovations to carry out in this regard.

- First, he writes that information resources have undergone a qualitative leap forward. This requires renovating and reorganizing information resources into system resources, dominant resources, and strategic resources. Information resources will dominate the entire process of war.
- Second, informationized forces have renovated the concepts of time and space mentioned earlier. It is now difficult to barter time for space since time processes in war have shrunk to such a great extent.
- Third, the forms of war and forms of operations must be renovated.
- Fourth the goals and objectives of war must be renovated. Now instead of focusing on annihilating the enemy, the focus must be on controlling the enemy. This means focusing on command centers, information systems, and information capabilities.

The psychological intensity of war has also risen.

- Fifth, weapon concepts must be renovated. EW, early warning, reconnaissance, and surveillance equipment must be made to act as one whole system in order to realize their potential overall effect.
- Sixth, combat strength assessments must be renovated. Objective assessments must be made of both sides' information capabilities and system structures. A comprehensiveness estimate of the warfare strength of the sides' operational systems must be made.
- Seventh, there must be a renovation in the concept of troop concentration. The focus now must be on qualities and not on numbers that emphasize only firepower concentrations.
- Eighth, combat support must be renovated. Measures must now be synchronized and real-time. The support system must be more centralized than before.
- Ninth, the composition of the armed forces must be renovated. Attention must be paid to the high-tech development of the Second Artillery, Air Force, and Navy even at the expense of ground forces.
- Tenth, the People's War concept must be renovated. Now there is more space into which People's War can be extended. The masses can still control the enemy as before but in a different fashion.[\[641\]](#)

Finally, informationized warfare must be accompanied by a change in the way war conductors think. For example, information deterrence is a concept that must be considered and developed further at the strategic level. It can help achieve national strategic objectives and military strategic objectives. Basic methods include information technology, information weapons, and information-resource deterrence. Counterinformation deterrence theories must also be considered.

Confrontations are moving in the direction of systemization. The fog of war created by information overload must be overcome by a complex system engineered for war thought. A commander's ingenuity is important but no longer sufficient by itself.[\[642\]](#) This has become so important in Yao's opinion that

If the assistance of electronic computers and artificial intelligence is taken away, the principals of war thought basically have no way of planning, managing, and responding to information age warfare. Only by achieving the optimal combination of the principals of war thought with electronic computers and artificial intelligence; utilizing a method of comprehensive systems integration; organically and completely integrating the information reasoning, analysis, judgment, strategy, and planning capabilities and experiences of the principals of war thought with information retrieval and storage, processing, transmission, and certain logical reasoning and judgment capabilities of electronic computer systems and artificial intelligence systems;... only then is it possible to greatly stretch and extend the functions of war thought and make it possible to solve the complex, huge, systematic problem of modern warfare.[\[643\]](#)

Yao states that war strategy has developed to the point where strategy is made technological and the use of technology is made strategic. Man-machine integration, strategy and tactics

integration, and leveraging tactics to carry out strategy are the points of emphasis. Any strategy that removes itself from the use of high-technology weapons has no useful value according to Yao. [644] This includes countermeasure weaponry

It is necessary to be proficient at utilizing the information superhighway, creating misleading information, spreading the fog of war, and jamming and destroying the enemy's strategic awareness, thereby using strategy to control the adversary. It is necessary to be proficient at using electronic feints, electronic camouflage, electronic jamming, virus attacks, and space satellite jamming and deception, leading the enemy to draw the wrong conclusion and attaining the goal of strategic deception.[645]

Asymmetric Warfare

Asymmetric warfare, in the opinion of the author of Decoding the Virtual Dragon, is one of the most often used, seldom defined, and misunderstood concepts in the US vocabulary. To date, the US military has still not defined the term in its dictionary of military terms. The PLA picked up on the term from its early use in the US and continues to write about the concept. Asymmetric war, to many US tacticians, implies the ability of a weak force to strike a strong force and perhaps therein lies its popularity to the Chinese. It has applicability and ties to ancient Chinese military history and their use of stratagems.

The PLA has defined asymmetric war in a host of ways. The most interesting, and most removed from any US understanding of the term, was provided by the journal China Military Science. A 2002 article stated that “asymmetric warfare is abnormal logic bringing together two sides that are pitted one against the other. It radiates the dialectic with 12 crafty tactics.”[646]

The chapter on asymmetric warfare in Warfare Strategy Theory defines asymmetric warfare differently which shows that they too are having trouble explaining the term. Initially editor Yao suggested that asymmetric warfare is war in which “there are great disparities in the numbers of the armed forces or distinctive superiorities and inferiorities in the quality of weapons of the antagonistic sides.”[647] Yao stated that it is not proper to believe that an “age gap” in weaponry can be called asymmetric warfare since it is not all that asymmetry implies. Viewing asymmetry from a comprehensive perspective, Yao then states that the fundamental meaning of asymmetry is

An imbalance in strength, so asymmetric warfare, simply speaking, is warfare in which there is a great disparity in the strengths of the two sides engaged in combat. Strength is the composite force that includes military strength and economic strength. The degree of strength is determined, generally speaking, by the differences in the industrial and technological levels of both sides.[648]

There is also a difference, Yao notes, between asymmetric operations and asymmetric warfare. Asymmetric operations consider methods of operations and forms of operations. It is a kind of measure taken to win an advantage in asymmetric warfare and falls in the campaign and tactics realm. Asymmetric operations refer to the side with weaker science and technology strengths calling upon its own strategy to curb the opponent, while the side with stronger science and technology strengths uses its own relatively superior science and technology to suppress the opponent.[649]

Asymmetric warfare, on the other hand, includes the initiation, conduct, and conclusion of wars. It is a category of warfare and is a part of the strategic level and must take into consideration factors such as politics, economics, culture, religion, psychology, geography, and weather. Asymmetric warfare is operational patterns for controlling strategic or campaign initiative while avoiding the enemy's strengths and attacking his weaknesses.[\[650\]](#) In this latter sense, Yao agrees with some US tacticians.

A superior side can initiate asymmetric warfare

- When it considers its own national interests absolute and magnifies them and encroaches on the national interests of a smaller country
- When it uses the values of strategic culture and superiority in a country's ideological makeup
- When it uses its lead in science and technology to its benefit (information technology has laid out a foundation for asymmetric war)
- When there are a lack of international arrangements for constraint
- And when the strong appear capable of defeating the weak.[\[651\]](#)

The inferior side can initiate asymmetric warfare

- When it adopts a strategy of limited aims/fait accompli
- When the inferior side has short-term offensive capabilities
- When it has the support of powerful allies
- Or when there is a change in the political power structure of a country or when extremist organizations and radical military organizations gain control of making policy.[\[652\]](#)

Yao also lists expected outcomes for the following types of clashes: direct offense of a superior force versus the direct defense of an inferior force (superior side wins), direct offense of a superior force versus the indirect defense of an inferior force (inferior side or indirect defense will win as long as it has sanctuary and society's support), indirect offense of a superior force versus the direct defense of an inferior force (superior force loses), and indirect offense versus indirect defense (superior side will win if it adopts brutal tactics).[\[653\]](#)

Yao lists characteristics of asymmetric warfare in the post-Cold War era. They are interesting and worthy of consideration. Yao initially discusses asymmetries between the forces of opposing sides. First, he states that there is now asymmetry in the principles of war. This is because instead of one country fighting another country, now we have countries fighting terrorists, drug cartels, and criminal groups. Second there are asymmetries in military strength due to the advancements in science and technology that some states have made as well as the economic support that some countries possess. Third, there is asymmetry in international support for operations where allies join in to confront a single country. Finally there is asymmetry in combat capabilities as a result of technology and economics.

Second, Yao notes that there is now asymmetry in operational space that is becoming more and more evident. The operational space of a superior side is increasing while that of the inferior side is decreasing. Further, nontransparency (superior side) and transparency (inferior side) of operational space exist side by side which gives even more initiative to the superior side.

Third, Yao states that increased asymmetry exists in time. Here he is referring to time spent on combat in general. While the superior side usually desires a quick decisive victory, an inferior side often wants a protracted conflict. In unconventional warfare the initiative is often controlled by the inferior side and time is on the side of the group that can drag out the conflict the longest.

Fourth, Yao states that combat is getting more and more diverse. Now analysts talk about mobile warfare, maneuver warfare, position warfare, noncontact and nonlinear warfare, and many other standard operations along with guerilla warfare, special operations, antiterrorism operations, and other nonstandard operations. Analysts also discuss virtual network attacks, economic warfare, and trade-embargo warfare among other issues. Yao recommends a close study of these issues. He notes that these new characteristics and rules are important for China to study and learn so they can capitalize on lessons learned by others who have preceded them.[\[654\]](#)

Conclusions

Yao's book is worthy of consideration as a solid source on contemporary Chinese military thinking with regard to warfare in general. This chapter only focuses on the informationization aspects of Yao's book and their relation to strategic issues. Yao implies that the relationship is quite important when he notes that "any strategy that removes itself from the use of high-technology weapons has no useful value."

Also of particular interest to the IW specialist is the spotlight Yao places on cognitive, systems, and control issues. System issues are discussed quite frequently in the Western military circles and do not require explicit attention here. But the cognition and control issues are less often discussed and merit our attention.

Both Dai and Shen stressed cognition and control in their earlier works so Yao's attention to them appears to continue a trend established a few years ago. Whether this is part of the strategy of "winning without fighting" is not known for certain, but it does fit that paradigm. If one can control the will and emotions of a foe or control the information that an enemy commander is receiving on the battlefield, then it will be much easier to conquer that foe. Even winning without fighting is a possibility. Dai covers the cognition element well in his discussion of network psychological war.

Control deserves a few more words, however. War control is defined as a "commander's implementation of restricting and limiting behavior on the occurrence, development, scale, strength, and end result of war." In the information age this can include the use of information deterrence measures to contain war. But other factors are also at work. Precision-guidance weaponry has become a tool to control war. Information technology has produced both battlefield and socio-political transparency, and this has increased control by placing every move under close scrutiny. Economic and technical means are now more effective than the use of direct military means to secure interests, and this has improved control.[\[655\]](#)

With regard to asymmetric warfare, perhaps informationization will become an important element of asymmetric warfare (or vice versa!). Many of the points that Yao stresses about informationization (the change in the importance of time and space, in the principles of war, and in the diversity of warfare) are also addressed in the asymmetric warfare discussion. This indicates a close link between the two. He recommends a close study of these issues and hopes that China can capitalize on lessons learned by others. The information-generated fog of war may, for example, be one of Yao's asymmetric methods of attack.

In short, even though Yao's new work does not offer much new in the area of informationization, it is nonetheless impressive for its breadth and depth of analysis of warfare. It is worthy of close examination by military specialists in general.

Warfare Strategy Theory
Yao Youzhi, Editor-in-Chief
2005

Table of Contents

Yao Youzhi: Editor-In-Chief
 Chen Yikang: Chief Editor
 Ma Debao, Yu Miao: Assistant Editors
 Publisher: Liberation Army Press
 Date of Publication: 2005

Introduction		1
Section I – Warfare Concepts		
Chapter 1	Warfare Concepts	1
(1)	Theoretical Analysis of Warfare Concepts – Compositional Elements and Current Circumstances	1
(2)	Actual Rules for Warfare Behavior – Circumstances and Indications of Warfare Start and End	8
(3)	Misconceptions about Warfare Concepts – Errors and Misinterpretations of the “General Discussion of the Theory of Warfare”	12
Chapter 2	War Motivation	
(1)	The Motivations for War Are Continually Developing.....	19
(2)	The Motivations for War Are Varied and Complex.....	23
(3)	Problems with Looking Historically at Motivations for War	27
Chapter 3	Warfare Force	34
(1)	War Is an Organized Confrontation of Force	34
(2)	Modern Warfare Developments and Resultant Changes to the Nature of	

	Its Force	37
(3)	Warfare Violence Characteristics and Manifestations	43
Chapter 4	Characteristics of War	49
49	(1) Western Justice Warfare	
	(2) Warfare Characteristics within the Boundaries of International Law	52
	(3) Theory of Marxist Warfare Characteristics	56
	(4) Questions of Justice in Current Warfare	58
Chapter 5	The Effects of War	68
	(1) The Effect of Warfare Is Historical	68
	(2) The Effects of Warfare Are Different because Its Characteristics Are Different	71
	(3) There Are Many Direct Effects of Warfare	75
	(4) Manifestation of the Effects of Modern Warfare is Changing	83
Chapter 6	War Objectives	88
88	(1) Connotations of Warfare Objectives and Their Relationship to the Purpose of War	
	(2) Primary Characteristics of the Objectives of War	93
	(3) Selection and Planning, Management and Control of Warfare Objectives	95
	(4) Reconceptualization of Warfare Objectives under Informatized Conditions	99
Chapter 7	Warfare Morality and Justice	102
	(1) Four Basic Positions on Warfare and Morality	102
	(2) Basic Principles of Modern Warfare Morality and Justice	108
120	(3) Contributions of the Chinese Government to Modern Warfare Morality and Justice	
	(4) Development Prospects for Modern Warfare Morality and Justice	123
Chapter 8	Warfare Victory and Defeat	128
	(1) Historical Evolution of Warfare Victory and Defeat Concepts	128
	(2) Challenges to Traditional Warfare Victory and Defeat Concepts	132
	(3) Establishment of New Types of Warfare Victory and Defeat Concepts that Embody the Characteristics of the Era	136

Section II – The Features of Warfare

Chapter 9	Forms of Warfare	148
(1)	Characteristics and Signs of Historical Forms of Warfare	148

	(2)	Features of Informatized Warfare	153
	(3)	Inevitability of Evolution of Warfare Forms	156
	(4)	Developmental Patterns of Warfare Forms	160
Chapter 10		Modes and Styles of Warfare	166
	(1)	Modes of Warfare	166
	(2)	Styles of Warfare	183
Chapter 11		Scale of Warfare	207
	(1)	Historical Trends of Changes in the Scale of Warfare and Determining Factors	207
	(2)	Principal Measurement Indices for the Scale of Warfare	209
	(3)	World War and Local War	211
	(4)	The Scale of High Technology Local War Is Becoming Increasingly Controllable	215
Chapter 12		Warfare Time and Space	219
	(1)	Warfare Time and Space and Associated Characteristics	219
	(2)	Important Effects of Recognizing Warfare Time and Space	226
	(3)	New Time and Space Characteristics of Informatized Warfare	229
Chapter 13		Warfare Structure	235
	(1)	Features of Prominent Structural Force in High Technology Warfare ..	236
	(2)	Warfare Systemization Is a Product of the Grand Development of Military Science and Technology	242
	(3)	Taking Hold of Structural Force Becomes the Core of Strategic Direction	247
Chapter 14		Asymmetrical Warfare	253
	(1)	Internal Rules for Asymmetrical Warfare	253
	(2)	Generation Mechanisms of Asymmetrical Warfare	256
	(3)	Outcome Analysis of Asymmetrical Warfare	261
	(4)	Features of Asymmetrical Warfare in the Late Cold War Period	265
Chapter 15		Nontraditional Warfare	268
	(1)	Boundaries of Nontraditional Warfare and Their Motivations	268
	(2)	Principal Types of Nontraditional Warfare	270
	(3)	Several Points for Consideration of Nontraditional Warfare	273
Chapter 16		Quasi-warfare	276
	(1)	Quasi-warfare and Its Forms	276
	(2)	Features of Quasi-warfare	279
	(3)	Differences and Connections between Quasi-warfare and Warfare	281
	(4)	Reasons for Frequent Incidence of Quasi-warfare	284
	(5)	General Guidance Rules for Quasi-warfare	286

(6)	Development Trends of Quasi-warfare	289
Chapter 17	Antiterror Warfare	291
(1)	Outline of Antiterror Warfare	291
(2)	Causes and Sources of Antiterror Warfare	296
(3)	Features of Antiterror Warfare	301
(4)	Development Trends of Antiterror Warfare and Effects of Antiterror Warfare on the International Structure and Security Strategy of Principal Countries and its Development Trends	304
Chapter 18	Nuclear Warfare	312
(1)	Basic Rules of Nuclear Warfare	312
(2)	Modern Nuclear Military Theory	320
(3)	Nuclear Warfare in the Information Age	323
Chapter 19	Informatized Warfare	328
(1)	Informatized Warfare Is an Historical Leap of the Shape of Warfare ...	328
(2)	Informatized Warfare Is the Abandonment of Traditional Warfare	337
(3)	Network-centered War Will Become the New Style of Informatized Warfare	346

Section III – War Preparation

Chapter 20	Concepts of War Preparation	350
(1)	There Is Serious Danger of War, and Strategic Concepts are Absolutely Necessary	350
(2)	War Preparation Is Related to National Security, and the Strategic Concepts of All People Are of Utmost Importance	352
(3)	The Side that Can Fight Can Also Hold Back the Fighting, Constant War Preparation Is the Army’s Iron Rule	356
(4)	Only Preparation Can Relieve Concern, War Preparation Will Always Be the Key	359
Chapter 21	War Planning	361
(1)	War Planning Basic Theory and Historical Experience	361
(2)	The “Network-centered War” Cannot Be Separate from War Planning	366
(3)	Information Technology Is the Mainstay of the “Star Wars” Plan	367
(4)	Modern Warfare Relies Even More on Well-Conceived War Planning	370
Chapter 22	War Power	374
(1)	War Power Operating Rules	374
(2)	Overall Structure of War Power	380
(3)	Basic Features of War Power	384
(4)	Quantification Assessment of War Power	388
(5)	Changing Trends of War Power	391

Chapter 23	Weaponry	394
(1)	Weaponry Emergence and Development are Important Driving Forces Needed for War	395
(2)	Technological Progress is the Decisive Factor in the Development of Weaponry	398
(3)	Scientific Weaponry Theory is the Guide for Weaponry Development	400
(4)	Promoting Ever Increasing Troop Combat Strength by Constantly Updating Weaponry	402
(5)	Weaponry Building Must Be Done Hand in Hand with Cultivation of High Quality Personnel	404
(6)	Relying on the Internal Impetus of Weaponry to Promote Development of Weaponry along the Right Path	407
(7)	The Development of Weaponry Brings New Military Transformations and Is One of Its Main Components	410
(8)	Controllable Weapons That Restrain War Such as Small-scale Nuclear Weapons Are Becoming Increasingly Important	412
Chapter 24	Combat Organization	416
(1)	Basic Theory of Combat Organization	416
(2)	Combat Organization in High Technology Warfare	421
(3)	Effect of New Military Changes on Combat Organization	428
Chapter 25	Rules of Warfare	432
(1)	Warfare Rules Have Demonstrated Civilization and Progress in Human Society	432
(2)	Warfare Rules Play an Important Role in Restricting War and its Perniciousness	435
(3)	Efficacy and Limitations of a Dialectical View of Warfare Rules	441
(4)	Application of a Correct Understanding and Grasp of Warfare Rules in Modern Warfare	445
Chapter 26	Mobilization of War	448
(1)	Practical Paths and Theoretical Evolution of War Mobilization	448
(2)	Problems Related to War Mobilization	451
(3)	New Models for War Mobilization in the Twenty-first Century.....	454
Section IV – Implementation of Warfare		
Chapter 27	Warfare Thought	466

466	(1)	The Essence of Warfare Thought and Its Significance for Warfare Guidance	
	(2)	Fully Revised War Concepts Must Be Implemented for Warfare Thought in the Information Age	469
	(3)	Basic Transformations in the Method of Thinking Must be Implemented for Warfare Thought in the Information Age	473
Chapter 28		Means of Warfare	481
	(1)	Force Is Still the Essence of Modern Warfare, but Shades of "Humanity" Are More Involved	481
	(2)	The Expansion of Modern Means of Warfare	484
	(3)	Operating Features of Modern Means of Warfare	487
Chapter 29		People's War	490
	(1)	The Essence of Mao Zedong's People's War Ideology	492
	(2)	People's Warfare Faces Opportunities and Challenges	492
	(3)	Innovation and Development of People's War Ideology	498
Chapter 30		War Assurances	504
	(1)	Historical Track of Logistical Assurances	504
	(2)	Logistical Assurances Are a Strategic Problem that Impacts the Success or Failure of War	508
	(3)	War Assurances Are Becoming Increasingly "Precise"	518
Chapter 31		Warfare Guidance	521
	(1)	Rules for Warfare Guidance	521
	(2)	Basic Links of Warfare Guidance	524
	(3)	Understanding New Warfare Rules	527
	(4)	Developing the Ideology of Warfare Guidance for China's Army	
530			
Chapter 32		Warfare Supremacy Theory	536
	(1)	The Concept, Component Factors, and Characteristics of Supremacy..	536
	(2)	Supremacy Theory and Its Evolution	538
	(3)	Interrelationships between Each of the Supremacy Theories	552
	(4)	Development Trends of Supremacy Theory	554
Chapter 33		Theory of Initial War Stages	557
	(1)	The Initial Stages of War Receive General Emphasis	557
	(2)	New Features of the Initial Stages of Modern War	561
	(3)	Only with Thorough Preparation Can the Right to War Initiative Be Won in the Early Stages of Conflict	568
	(4)	Evaluating the Military Strategy of "Gaining the Initiative by Striking First"	570

Chapter 34	War Control Theory	572
(1)	War Control and Its Relationship to Local War	572
(2)	The Origins and Evolution of War Control Ideology	574
(3)	The Premises and Conditions of War Control	577
(4)	Principal Content of War Control Theory	581
(5)	The Significance of War Control Theory	584
Chapter 35	War Conclusion Theory	588
(1)	War Conclusion Content to Be Studied	588
(2)	Restrictive Factors in the Conclusion of War	592
(3)	General Principles of War Conclusion	595
(4)	Basic Principles of Conclusion of High Technology Local War	598
Chapter 36	Benefits of War	603
(1)	Boundaries of the Benefits of War	603
(2)	Principal Factors Affecting the Benefits of War	606
(3)	Pursuit of War Benefits Is an Objective Requirement and Necessary Trend in Economic and Military Development	609
(4)	Controllability of Modern Warfare Makes Pursuit of Comprehensive Benefits Possible	612
(5)	Innovation Is the Basic Path for Pursuit of Optimal Comprehensive War Benefits	614
Chapter 37	Arms Theory	618
(1)	Historical Development of Arms Theory Cognition	618
(2)	Foundation for the Consideration of Arms Theory	625
(3)	Predicaments and Directions of Arms Theory Practice	631
Primary References	643

CHAPTER TEN: CONCLUSIONS

Decode: 1. to convert into intelligible form. To recognize and interpret. 2. decipher. To discover the underlying meaning of.[\[656\]](#)

Introduction

The development of military affairs in the twenty-first century has caused Chinese theorists to rethink how to apply stratagems and strategy. The main causes of change were the recognition of the impact of information and system technology and weapon miniaturization on military affairs.

The information factor has offered a new vector for Chinese military pursuit. In recent Chinese White Papers on national defense this vector was described as the requirement to informationize the armed forces. The [2006 White Paper](#), for example, stated that the RMA is developing worldwide and, based on informationization, military competition is intensifying. The [White Paper](#) added that informationization will be used as the main criteria to measure the qualitative improvement of the People's Liberation Army (PLA); that for China to build a strong defense, it must build informatized armed forces and be capable of winning informatized wars by the middle of the twenty-first century; and that the PLA has built virtual laboratories, digital libraries, and digital campuses to support the training and teaching needed to field this informatized force.[\[657\]](#)

The mission of [Decoding the Virtual Dragon](#) was to illuminate for the Western reader Chinese thinking on these changes and how the PLA is integrating them into the force as the PLA transforms from a mechanized to an informationized force. This was accomplished in three stages. First, there was a discussion of the Chinese definition of strategy (its basic and applied aspects) and how information warfare/information operations (IW/IO) fits into the PLA concept of military science, specifically into the science of information operations. In a similar fashion, there was a discussion of how the revolution in military affairs, which is information-technology based, affected strategy. Second, there was an examination of two books regarding information operation concepts that were not available to this author when his first Chinese IW book, [Dragon Bytes](#), was published. That examination covered the 1999-2003 period and discussed some of the concepts and first steps to teach the force about information technology's (IT's) impact on military affairs. Finally, there was a review of three works from 2004 through 2006. One explored how China views network-centric warfare in the US and in China. The second examined a host of terms that are defining informationization issues. The third looked at Major General Yao Youzhi's 2005 perspective on warfare strategy. These works indicate how IO has taken hold of military affairs in China.

In the course of the investigation, a number of issues were raised that shed greater light on these Chinese concepts, their integration, and potential meaning. It is the purpose of this chapter to consolidate these items into eight key issues and some final thoughts. In this manner it is hoped that one can decode or "convert into intelligible form" what Chinese IO is all about and how it fits into a larger geo-strategic picture for the PLA.

Exploring Components of the Strategy-IO Relationship

One of the key lessons of this research was discussing the difference in how US and Chinese military professionals define strategy. Strategic studies are looked upon by the PLA as cognitive activities. In this endeavor Chinese military academicians still utilize Marxist cognitive methods, believing they provide a golden key to analyze strategic problems comprehensively, dialectically, objectively, systematically, continuously, concretely, and connectedly.[658] This implies that methods of stratagem confrontation; methods of prediction; and methods of experiment and simulation are used.[659]

In stratagem confrontation the subject must confront the enemy through strategic activities with better wisdom. He must analyze truth and falseness, compare strength and weakness, and employ orthodox and unorthodox tactics via dialectics. Stratagem is made up of dialectics, logic, math, and other scientific methods. In methods of prediction, one must make correct inferences or judgments based on knowledge of the objective laws of war. Methods of experiment and simulation are important means of coming up with an analytical judgment and, therefore, strategy. [660] Cognitive activities thus become the indirect method to defeat an opponent.

Chinese strategists emphasize objective and subjective factors as a focal point and way of viewing and applying strategy. US professional do not use this technique. While the Chinese attach great importance to the substance and laws of war, they attach equal importance, it appears, to the application of subjective creativity to objective conditions.

Objective conditions include the distribution of forces, defense budgets, level of science and technology, the economy, politics, military power, and the general potential of nations to generate power. These are some of the criteria a war conductor or strategic commander must consider in the development of strategy.

Subjective creativity applies experience and knowledge to these objective conditions in the form of strategic judgments and decisions. The characteristics of strategic thinking include totality (comprehensive look at the parts and elements), confrontation (contest of material and spiritual forces), certainty (start with the fact that war is full of uncertainty about the enemy situation but end with certain conclusions about the enemy), foresight (use history, current factors, wisdom, and resolution to visualize future war), creativity (the soul of strategic thinking requires subjective initiative to surpass experience and tradition), and inheritance (culture). It takes into consideration the subjective will of the opponent. When subjectivity is applied to objective conditions the result is the creation of strategy. The Chinese war conductor attempts to find ways to creatively manipulate, deter, or overcome deficiencies and exploit opportunities.[661]

This objective-subjective prism has become the basis for many Chinese definitions or explanations for war and strategy. For example, the Science of Military Strategy notes:

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 conductor's personally 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 having a bearing on war strategy and reveal their inherent connections with war strategy.[662]

Mao as well noted that war is a contest in subjective ability between commanders of opposing armies for the initiative and attainment of superiority on the basis of material conditions such as military forces and financial resources.[663]

Yao and Peng subdivided the science of military strategy into basic and applied theoretical aspects. In the basic theory field of the strategy of military science, they listed a host of factors that defined objective conditions. Some were situational, some material, some cultural, and some ideological. These factors included:

- National interests, war strength, and war potential of opposing forces
- International and domestic political situations (the international political configuration, international coalitions, and international organizations)
- The strategic intentions of major states
- The overall balance of power
- The influence and restrictions of domestic politics[664]
- Geo-strategic relationships
- Natural geographic elements (a state's geographic position, size and shape of territory, natural resources, national capital, frontiers and national boundaries, distance between states, and grand strategic space)
- Human geographic elements
- Vital interests between states, interests of nations, and religions
- Various strategic alliances
- Geo-economic relations[665]
- And a comprehensive view from various aspects and stages (space, time, etc.).
[666]

The applied aspect of theory is the actual application of thinking to basic criteria. This includes the formulation of strategy (judgment, planning, decision making), and performance of strategy (guidance for the employment and construction of military forces). In general these issues included in their explanations both objective and subjective criteria. For example, Peng and Yao wrote that strategic command is based on the objective reality of war. This refers to all the objective conditions such as combat forces, battlefield posture, space-time environment and command system, and spiritual factors such as consciousness, morale, and the feelings of the troops. Subjectivity is the directing and waging of war and man's conscious dynamic role in it. Subjective efforts become an important manifestation of the strategic art of command.[667]

Even for concluding a war it was noted that objective and subjective factors are important:

There are subjective and objective implications for the timing of concluding a war. Objectively, it means that war has developed to a certain extent and satisfies the conditions for its conclusion within a certain timeframe. Subjectively, it means the choice made by the war conductors on the timing for concluding the war according to changes in war conditions.

To end the war, objective conditions and proper timing are equally important.[668]

There are, of course, alternate Chinese definitions and explanations of strategy for the reader to consider. One source that can be considered as authoritative, at least in its open source (publicly available) nature, is the Chinese Military Encyclopedia. It defines strategy in the following way:

Strategy is the analytical judgment of such factors as international conditions, hostilities in bilateral politics, military economics, science and technology, and geography as they apply to the preparation and direction of the overall military/war plan. It is advantageous: to study the occurrences and developments in war forecasting/predictions; to formulate strategic policy, strategic principles, and strategic plans; to make warfare preparations; and to put into place directives on the actual principles and methods of warfare.[669]

In brief, the encyclopedia states that strategy is an analytical judgment of how certain factors apply to the preparation and direction of a war plan. It does not appear to emphasize objective-subjective conditions except in a circumstantial way.

A **second** key issue of this research was discovering how the PLA's definition of IW and IO has changed through the years. This point can determine how information-based equipment is applied in conflict or battle and is worthy of examination. Chapter One of the book Dragon Bytes covered this item extensively for the years 1999-2003. Major General (retired) Dai Qingmin's Direct Information War was written and published during this time period but was unavailable to this author when Dragon Bytes was written. It was covered in this volume since it offered one more definition for both IW and IO. The 2005 book he directed, Study Guide for Information Operations Theory, offered yet another more updated definition of IW and IO. One can see from the discussion below that the definition of the terms (with Chinese characteristics) is progressing.

In his 2002 work Direct Information War, Dai defined information war in the following manner: "This term refers to the use of computer network systems to gain enemy intelligence and destroy enemy systems in order to improve the military's defense and attack capabilities as well as the intelligence capabilities of one's own side...it is attacking the enemy's 'nervous system' with viruses and various long-range control measures, paralyzing the computer network system of his headquarters, or entering wrong intelligence and wrong commands into the enemy's military command system, thereby reaching the goal of victory in war." [670] The work in which this definition appeared was about network warfare.

In the 2005 Study Guide for Information Operations Theory, Dai and his co-workers defined information war quite differently:

Information warfare first appeared as an item in Military Terms Used by the People's Liberation Army of China published by the Academy of Military Sciences in September of 1997. It was defined as 'countermeasure activities in the information realm performed by two sides in a conflict, primarily in contending for information resources, in gaining the initiative in the production, transmission and processing of information, and in destroying the enemy's information transmission as a means of creating favorable conditions for containing

or winning a war.’

Information warfare is a broad concept, and is defined in both broad and narrow senses. The broad sense of information warfare, also known as strategic information warfare, refers to countermeasures and combat using information and information technology by two sides in a conflict as a means of gaining information superiority in the areas of politics, the economy, science, technology, diplomacy, culture, and the military, both in the civilian and military realms, during peacetime or in times of war, either on the battlefield or off of it. The narrow sense of information warfare is that it is the information countermeasures performed in the information realm by two sides in a conflict as a means of gaining information superiority, i.e. what the US military calls ‘battlefield information warfare.’ The narrow sense of information warfare manifests itself mainly in the form of intelligence warfare, electronic warfare, network warfare, and psychological warfare. It is developed on the foundation of electronic warfare, which is supported by electronic technology. It is, in the main, still electronic warfare. The broad and narrow senses of information are not completely distinct from each other, but are often intertwined, each advancing and acting upon the other.

The more consistent view holds that information warfare consists of military countermeasure actions using information operations and other related operational powers to achieve and maintain information superiority. The definition currently employed by the Chinese military typically uses the narrow sense of information warfare.[\[671\]](#)

There are three points of importance in these definitions. First, the Direct Information War definition is offensive, designed to destroy enemy systems to improve one’s attack capabilities, and it is targeted against network systems and includes deceiving the enemy’s system as much as possible. Second, the Study Guide for Information Operations Theory definition of IW is not as offensive oriented, stating simply that countermeasures using IO are necessary to achieve information superiority. This reliance on countermeasures is recounted in all of the definitions (broad and narrow) offered by Dai and will require further investigation by analysts as to what this means. Finally, Dai and his coworkers break IW into strategic and battlefield IW. Strategic IW includes “politics, the economy, science, technology, diplomacy, culture, and the military, both in the civilian and military realms, during peacetime or in times of war, either on the battlefield or off of it.” Battlefield IW includes “intelligence warfare, electronic warfare, network warfare, and psychological warfare.” This latter definition, of course, is close to how the US defines its IO capabilities.

While these definitions are recent, it would be remiss not to mention how the Chinese Military Encyclopedia defined IW. In this case, IW appeared in a year 2000 addendum to the original 1997 version. Here IW was defined in the following way (the complete entry, plus other IW related entries in the Chinese Military Encyclopedia are listed in Appendix Two):

Information Warfare [xinxizhan]- Operations carried out to seize and maintain information supremacy (FBIS translators consulted for this definition defined this term as control instead of supremacy). According to the time, it can be divided into peacetime information warfare and wartime information warfare. Peacetime information warfare refers to commonly conducted hostile, two party information confrontation in periods of peace in areas such as

politics, economics, science and technology, foreign relations, culture, and military affairs. Wartime information warfare refers to hostile, two-party information warfare carried out in periods of war. It includes using many kinds of measures to attack the enemy's information and information systems; to damage or sever the enemy's flow of information; and to influence, weaken, or destroy the enemy's information operations capabilities, while safeguarding the information operations capabilities of one's own side. Information warfare includes two mutually connected aspects, and those are information attack and information defense.[672]

Dai apparently used an aspect of this definition in his 2005 work.

In Direct Information War Dai defines IO in the following manner: “This is the general designation for the various operational activities and measures carried out to weaken or destroy the useful efficacy of the enemy’s information systems on the battlefield, to include ensuring that one’s own information systems retain their efficacy. It is an important component in joint operations, it stands side by side with firepower and mechanized power as a third attack measure, and it is also the prerequisite and the basis for capturing the battlefield initiative.”[673] These operational measures have designated operational goals, operational objectives, and operational forms. Here Dai limits his description to simply operational activities and measures (the latter has goals, objectives, and forms) to weaken or destroy enemy systems.

In Study Guide for Information Operations Theory, there are several definitions of IO. They appear to be an attempt to list how the definition has progressed over time. Dai and his coworkers note:

At present there are three main definitions for information operations. The first is as follows: ‘Information operations refer to operations used to gain and maintain control over information.’ This definition expands the domain of information operations, as there are quite a few ways to gain and maintain control over information. Second, ‘Information operations refer to a series of operational actions employed by two sides in a conflict in which the enemy’s information systems are used or destroyed and one’s own information systems are protected as a means of gaining the power to acquire, control, and use information.’ Third, ‘Information operations refer to a series of operational actions undertaken to gain and maintain information superiority on the battlefield or control over information. The two sides in a conflict use electronic warfare or computer network warfare to use or destroy the information and information networks of the enemy and protect one's own information networks as a means of acquiring, controlling, and using information.’

An analysis of the three points given above reveals the two major goals of information operations: the first is to destroy the enemy’s information and information systems while protecting one's own; the second is to destroy the enemy's cognition and beliefs while protecting one's own. This fully explains why information operations are not comprised only of electronic warfare (the use of information media, i.e. signals, to destroy information transmissions), but also include computer network warfare and psychological warfare (the use of the content of information to destroy information systems along with human cognition and beliefs).

It is clear, then, that the targets of information operations are information, information systems, and the cognition and beliefs of people. The means employed in information operations include information (both information media and information content) and weapons and equipment dedicated for attacks on information systems. Information operations involve both attacking and defending.[674]

One item common to all three definitions is the requirement to control information. From a look at these definitions, control appears more important than supremacy. The emphasis in the last paragraph on cognition and beliefs is also a point to take seriously, as this was also listed as a key aspect of understanding strategy.

But Dai and his coworkers added one more definition of IO and it is the last one known to this author as this book goes to press (no definition of IO was listed in the Chinese Military Encyclopedia). The description lists the targets of IO (information, information systems, and the cognition and beliefs of people) and the means employed (information [both information media and information content] and weapons and equipment dedicated for attacks on information systems). This definition of IO states that:

Information operations are defined as a series of countermeasures employed by two sides in a conflict in which information or weapons and equipment controlled by information and dedicated to the destruction of information systems are used in order to influence and destroy the enemy's information, information systems, and cognition and beliefs, along with preventing the influence and destruction of one's own information, information systems, and cognition and beliefs in the same manner by an enemy.[675]

Again, just as in the definition of IW, countermeasures are used in the definition. Further, it is stated that information, weapons, and equipment must be controlled by information but dedicated to destroying information systems while protecting Chinese systems. The items of countermeasures and control are absent from US definitions and probably are worthy of further investigation by analysts.[676] The issue of countermeasures will be covered in the section on *Final Thoughts* below. The US focus in IO has been on information supremacy, influence operations, and other means while US targets are similar to Chinese targets (systems, etc.). Only the Chinese recognition of cognition and beliefs as separate items serve as a point of variance in target sets. US analysts, of course, argue that psychological operations are the equivalent of cognitive actions.

Integrating Strategy and IO

The **third** key issue of this research was discovering the extent to which Chinese authors described the integration of strategy with the influence of IW, IO, and information technology. Peng and Yao noted that the PLA must be “guided by the principles of military strategy in the new era to bring forth new ideas to push ahead the principles of strategic actions for local war under high-tech conditions...”[677] This strategy-IO or strategy-technology integration was also highlighted by other authors. Perhaps the most notable comments were made by IW specialists Shen Weiguang and Dai Qingmin. Shen noted, “The issue of information and network security, which accompanies the development of informationization, and the rise and increasing prominence of information warfare, the form of warfare that is invisible and non-violent, is an issue of technology, **but above**

all else it is an issue of strategy.”[678]

Dai offered a similar statement about the importance and probability of an IW/IO-strategic integration. He noted that “Laying all one’s hopes on technology is dangerous. The road to future losses may not be from a fall in technology, it may be primarily poor strategy. In reality the informationization of the forms of warfare has opened up an even broader space for playing tricks and using strategy and for using the indirect to gain the upper hand.”[679] Even conditions of technological superiority will not allow for success in all cases if strategy is overlooked according to Shen and Dai. Of course such thinking also coincides with traditional Chinese thinking and with viewing a situation from a position of being the weaker of two contestants in a battle.

IO has provided the PLA with a new means for applying strategy, one that enables a new information-based use of manipulation, deception, and soft (computer) destruction as much as hard (physical) destruction. Noted strategist Li Bingyan offered the best example. He made three observations: first, how too much information can be blinding and prohibit or stilt strategy; second, how there is a way for weak information technology nations to successfully attack strong information technology nations with the use of stratagems; and third, information technology can serve strategy as an effective deterrent and prevent war from ever breaking out. These are direct examples of how IO and strategy are being integrated into Chinese thinking.

In addition to Shen, Dai, and Li, other concepts that fit the strategy-IO paradigm were explained in The Science of Military Strategy. These concepts were the result of how information affected applied theory. For example, Peng and Yao, writing about the strategic maneuver aspect of applied theory of strategy, stated that the struggle in the information field may lead to changes in strategic maneuver. In particular, a “strategic information operations force may become a new form of strategic maneuver in future wars.”[680] If such a type of maneuver actually does develop, then other questions must also be explored in the applied theory arena. Will there be cyberflanking, cyberpenetration, and other cyber activities? One would think so based on the articles that have appeared in authoritative Chinese military journals. For example, it was the China Military Science article noted in Chapter Four that listed several types of IW stratagems for use in the information age.

A **fourth** key issue is the Chinese focus on a comprehensive approach in the broadest terms. As noted in Chapter One of this work, China tends to view many concepts from a comparative comprehensive framework just as they do in their CNP analysis. Those items listed in Chapter One were:

- Comprehensive national power (CNP)
- Comprehensive sea power (CSP)
- Comprehensive strategic interest (CSI)
- Comprehensive strategic targets (CST)
- Comprehensive strategic benefits (CSB)
- Comprehensive cyberized war (CCW)
- Comprehensive confrontation capacity (CCC)

- Comprehensive national defense construction (CNDC)
- Comprehensive support efficiency (CSuE)
- And comprehensive national strategy (CNS).

CCW represents the most significant integration of strategy and IW. There are comprehensive comparative lists in other publications as well. The 2006 Chinese White Paper on National Defense, for example, used the term “comprehensive” fifteen times in describing its national defense posture.

The Chinese method of viewing objective factors of power comprehensively is different than the methodology used in the US to measure power. While the Chinese CNP method uses nine or so elements to develop a power rating, the traditional US focus has been on diplomatic, information, military, and economic (DIME) issues; or more recently on political, military, economic, social, information, and infrastructure (PMESII) parameters for an understanding of power.

It is instructive for US analysts to learn China’s CNP methodology for predicting their national power assessments. Otherwise, how would a US analyst understand a Chinese strategic perspective that is influencing the latter’s thinking? It is worthy of note, however, that this is not a military assessment of Chinese power, just a civilian assessment. The military assessment would likely include other parameters of which we are not aware at this time

Integrating technology into strategy may also generate new ways for computing the CNP of China and other countries. It is an interesting subset of the integration topic and should be considered further from the perspective of its strategic framework. CNP is a holistic way of looking at objective factors that might be creatively influenced in an IO or technical way. Competition would thus not be looked at by the Chinese in a typical US bipolar pattern but rather in a manner involving comprehensive national power (CNP) issues.[\[681\]](#)

An example of CNP (and indicator of how important IO has become to CNP and strategy) is implied by a product known as the 2006: World Political Security Report (Yellow Book of International Politics). It is a Chinese work that, among other things, takes a look at the Chinese concept of comprehensive national power. Wang Ling wrote a chapter titled “Comparative Studies of the Comprehensive Power of Major World Countries.” In it he asks, “How does international power look at the beginning of the century?”; “How does China’s comprehensive power compare with other major countries?”; and “How do you determine the criteria for assessing the strength of individual countries?”[\[682\]](#) For examining national power, Wang’s assessment looked at science and technology, human capital, capital resources, information power (he focused on infrastructure), natural resources, government regulatory power, military power, diplomatic power, and economic power.[\[683\]](#) Wang’s assessment could also be considered a look at the world’s objective conditions. Naturally, subjective creativity (strategy) could be applied against this outlook to manipulate the conditions and factors exposed by the analysis.

When examining the civilian information infrastructure, Wang included factors such as computer users, Internet users, broadband users, number of mobile phones, fixed telephone trunk lines, and passenger loads for major airlines, highways, and railroads. The number of Chinese mobile phones per thousand households in 2003, for example, was stated as 214.8 versus 545.8

mobile phones per thousand households in the US.[684] These figures indicating a huge US lead are quite misleading in a comprehensive sense since we don't know how many households are in China and how many in the US.

Instead of using households, let's use a figure we do know, the population of both countries, and apply the criteria of the numbers for mobile phones per thousand households against it. Using 1.3 billion Chinese versus 300 million Americans, the number of total Chinese mobile phone users (214.8 mobile phones per thousand people in China) would be 279 million versus 164 million US mobile phone users (545.8 mobile phones per thousand Americans) or close to twice as many in China. A recent Wall Street Journal article noted that China now has 450 million mobile phone subscribers or more than one per person in the US.[685] The clear Leninist characterization here is that quantity still has a quality all its own. When examining numbers in China analysts must be prepared to extrapolate what Chinese percentages mean across the spectrum of this massive population.

Further, as high-tech conditions continue to advance by leaps and bounds, information production modes will keep on developing and global integration will move forward. Simultaneously, a new pattern (as Peng and Yao call it) of comprehensive cyberized war will appear.[686] This could imply that one takes an objective snapshot of the world's information resources and connections and then subjectively decides how to creatively conduct reconnaissance, manipulation, and destruction of these assets; or that the point of informationized war is to weaken or destroy the command and control systems of an enemy, the primary task of IW, IO, or NCW. In this way the initiative can be captured on the battlefield and the enemy's strategy can be disrupted.[687] IO doesn't just assist friendly forces' strategic interests, it can also be used to offset an enemy's use of strategy by destroying or disrupting his information technology.

A **fifth** key issue is the Chinese focus on strategic information. When discussing IW above, it was noted that in the broad sense, IW refers to strategic information warfare and that IO was a subcomponent of IW. Peng and Yao stressed the importance of good strategic guidance when developing and implementing strategic information operations. They noted that information superiority and information dominance must be maintained in order to keep the battlefield initiative and bring the power of information systems and cyberized weapons to bear on strategy. Operations must remain integrated if one desires to defeat an opponent in a system versus system confrontation.[688]

Peng and Yao list five types of strategic information operations. They are:

- Intelligence warfare—this type provides support for making decisions, and it can be divided into intelligence reconnaissance (space, network, etc.) and intelligence protection (information security).
- Command and control warfare—this type uses various means to attack an enemy's command and control element and destroy his information flow. This is the primary task of IW/IO whose essence is to capture the battlefield initiative
- Electronic warfare—this type's purpose is to seize electromagnetic command on the battlefield. Attack, defend, and support are three types. Space electronic warfare is a potential future method

- Cyber warfare—this type consists of soft kill (damage or destroy computers and networks) options and is a new operational pattern consisting of attack and protection
- Destructive warfare of information sources—this type consists of hard kill options (precision-strike cyberized weapons that destroy C4ISR and other relevant systems).
[\[689\]](#)

The Theme of Collecting Technical Parameters and Preemption

A **sixth** key issue of research was the continued Chinese emphasis on collecting technical parameters and developing preemptive attack plans, subjects also noted in [Dragon Bytes](#). The Chinese collection of US technical parameters is probably the one factor most often reported in the US press. Titan Rain and China's computer operations against the Naval War College are examples of this collection effort. Peacetime collection of information of US sites via reconnaissance allows China to prepare attacks against US vulnerabilities in the event they will ever need them.

When technical parameters of other systems are collected, countermeasures to them can be constructed as a sort of asymmetric response. China's [2006 White Paper](#), when discussing army projects, noted that information countermeasure units were one of three units that required priority development.[\[690\]](#) The primary reason behind the development of this force may have been to construct IW countermeasures.

The US launched reconnaissance in the form of electronic warfare and intelligence warfare more than six months before the Gulf war began the Chinese note. Such US actions are in line with Sun Tzu's concept that "the clever combatant seeks battle after the victory has been won." This implies that China's vision of future war will first involve information reconnaissance to collect technical parameters. This will ensure victory before the first battle. Reconnaissance consists of electronic warfare, radar, radio technology, and network reconnaissance. This concept of reconnaissance in peacetime fits perfectly with Dai's preemption concept and Sun Tzu's stratagem.
[\[691\]](#)

Dai noted that there must be a focus on collecting technical parameters and specific properties of information weapon systems and electronic information products. This, combined with his focus on information attacks, implies a preparation for preemption. Computer network reconnaissance is viewed by the Chinese as a prerequisite for victory in warfare. It helps them choose which opportune moments, which places, and which attack measures will result in maximum success if war ever breaks out.

When discussing preemption, Peng and Yao, for example, stated that IO is directly linked to the gain or loss of the initiative in war and thus "priority should be given to the attack and combining the attack with the defense." Information technology has enhanced Chinese thinking with regard to preemption. Chinese military academics state that those who do not preempt lose the initiative in what may be a very short-lived IO war. Combatants in present day conflicts find it easier to obtain the objective of war through one campaign or one battle than at any other time in history. The idea of sudden attack has changed. It doesn't mean "surprise" in the old sense but

rather that one side can't correspondingly react even though the situation is known. This is because one side possesses high-technology equipment and the other side only low-technology means. As a result preparation and mobilization are more important than ever before.[692] War preparations must be made ahead of time (to include the recruitment of information talent) to ensure that, if needed, an IO can be conducted suddenly with the use of all civil-military links.[693] Launching preemptive attacks to gain the initiative includes "striking the enemy's information center of gravity and weakening the combat efficiency of his information systems and cyberized weapons." [694] This allows one to weaken the enemy's information superiority and reduce his holistic combat efficiency.[695]

General Dai, writing in 2003, also noted the importance of carrying out information attacks. Whoever controls information supremacy controls war initiative in Dai's opinion.[696] Whether this process will only serve campaign planning and the acquisition of information supremacy or will be the manner in which China initiates an information attack in general is not known. However, Dai did write that IW has five natures and the first of these natures is that IW is precursory (begins before other operations) and whole course (runs throughout an entire operation). Perhaps the current emphasis on gaining the initiative and on short wars that are over quickly are the main reasons that Dai gives the impression that preemption via IW is a necessity in future war.[697] He notes that

Actions such as intelligence warfare, psychological warfare, and campaign deception in advance of combat seem to be even more important to the unimpeded implementation of planning and ensuring war. For this reason, information warfare must be started in advance of other combat actions before making war plans and while making war plans.[698]

Weak combatants, on the other hand, are unable to conduct such preemptive attack preparations. They must make good strategic preparations and organize to take quick actions against an enemy. Full play must be given by weak opponents to human subjective initiatives and the use of cost gap measures to counteract such a technology gap.[699] Clearly the observation is that the superior side uses technology to preempt when conflict appears imminent while the weaker side must employ subjective creativity to offset these attacks. A constant tension is thus established between strategy and technology in this regard.

In a sense, the Chinese note, it is the special features of IO tactics and techniques that enable the increased emphasis on attack more than traditional ground, sea, or air warfare. A weaker force, for example, can inflict much damage on a superior force with a properly timed and precisely defined asymmetric information attack. Such an attack may not be possible by traditional means. Multiple information attack actions must be adopted, the offense must be considered as defense, and information barrier methods must be developed by weaker opponents. Attack tactics include information deterrence, information blockade, information power creation (electronic camouflage, network deception, etc.), information contamination, information harassment, nodal destruction, system paralysis, and entity destruction.

China's specific understanding of the intersection of strategy and information technology, especially as it relates to conflict, is not terribly extensive in a practical sense due to a lack of recent experience with conflict. From a theoretical perspective, however, China has written

extensively on the use of information technology and preemption and given both much thought.

1999-2003 Books

A **seventh** issue discussed in Decoding the Virtual Dragon was the additional material from the 1999-2003 time period not available when Dragon Bytes was written. Dai Qingmin, in the 2002 work Direct Information War, focused primarily on the importance of networks and C4ISR. He also stressed quite dramatically the importance of cognitive activities. As a Chinese IO superstar, Dai's emphasis on this latter factor is important. For example, he noted that

Network warfare will rise from its current focus on confrontation on the physical level and logic level to confrontation on the super-logic level and that is the level of perception. The computer field will penetrate deeply into the thought processes of the human brain, influencing the spirit, morale, and consciousness of the adversary, disturbing the adversary's decision making mentality and the direction of decision making, forcing the enemy to give in to our intentions and demands, and forcing the enemy to submit by not fighting or by "psychological warfare."[\[700\]](#)

Dai believes that technology can be used to influence perception. He stated that electronic camouflage uses electromagnetic, opto-electrical, and thermal technological measures to simulate and duplicate the environment and make friendly targets blend in with their background. This "hides what is true" and "displays what is false" about the target. It can help thwart enemy electronic attacks and protect one's own systems. Metal foil strips, angular radar reflectors, colored smoke screens, plasma, multifrequency electromagnetic screens, photochromatic coatings, and optical bait are examples of measures that can deceive or change how one understands reality. Smoke camouflage now includes smoke made up of metallic chemical compounds and plasma which, when mixed with certain polymer ratios, makes smoke screens that can fluctuate to be consistent with the target and its background.[\[701\]](#)

Dai also explained his concept of network psychological war (NPW). NPW combines traditional psychological warfare thinking with modern network information technology. This type of warfare has several characteristics. It can transcend the nature of time-space according to Dai. It cuts across national boundaries (space) and can take place in peacetime or wartime. It can influence people's awareness and feelings in many fields, to include politics, economics, culture, and military affairs via propaganda, intimidation, deception, enticement, bribery, and deterrence. One of the methods to achieve these aims is to establish websites for psychological warfare and publish all types of deceptive, disturbing, leading, and deterring information. The idea is to disrupt normal judgment, block other information channels, and create misconceptions in the enemy.[\[702\]](#)

However, network warfare could develop in the direction of "network deterrence" or "network containment."[\[703\]](#) Bit streams in network space now control, Dai notes, not only the collection, transmission, processing, and distribution of information but potentially the thinking of command decision makers and operational personnel. Operational objectives of network space can now orient on the will, feelings, and cognitive processes of an enemy according to Dai.[\[704\]](#)

In addition to psychological/cognitive themes, Dai mentioned the potential for introducing a computer virus into the C4ISR system of an opponent, a method that may become a significant way

to conduct IW. Network warfare of this type is designed to attack the brain of the enemy's C4ISR system, according to Dai, and this affects strategic decision making and the overall strategic situation.

Dai added that integrated network-electronic warfare (INEW) shapes battlefield information warfare. It can also be called physical IW.[\[705\]](#) INEW allows operational secrecy, military deception, and psychological warfare to fuse.[\[706\]](#) This implies that science and art, strategy and tactics, and enticement and concealment are integrated creatively.[\[707\]](#)

Dai recommended establishing a new national security concept suited to the information age, one that elevated network-based strategies to the level of a national security plan. He advised speeding the pace of informationization within the country as a whole and speeding the establishment of rules and laws for an information network-based security regime. He added that controlling the initiative in war and destroying the adversary's operational intentions will enable Chinese forces to control the course of the development of a war. This must be the operational standard for network warfare forces.[\[708\]](#)

Shen, on the other hand, focused mainly on the issue of information security in his 2003 work Deciphering Information Security. Of particular interest in his work was the creation of an Information Security University. The university was laid out in great detail and had an extensive military orientation, with an added military specialty of economics.

2004-2006 Books

An **eighth** issue was the discussion of three books written after the 2003 timeframe. There is less to say analytically about these books since much of what the Chinese wrote was simply their interpretation of US network-centric warfare (NCW) doctrine or, in the case of Study Guide for Information Operations Theory, simply discussing Chinese terms.

The key points from An Interpretation of Network Centric Warfare are listed here. Selected chapters from this text were used to prepare this summary. Specifically, the chapters on weapons integration, C4ISR, battlefield management, and the book's concluding chapter which discussed the Chinese version of NCW were used. The following were the key findings from a Chinese perspective:

- C4ISR is NCW's foundation, a key tool in future war due to its fusing and force multiplier effects, and thus its security will always be an issue.
- A C4ISR system architecture has three layers: an overall structure, a service C4ISR system structure, and a functional element structure. Frameworks are studied from the perspective of operations (tasks), systems (capabilities and characteristics), and technology (a minimal set of rules governing the relationships among system components).
- NCW allows strategists to directly monitor events at great distances and sometimes control tactical actions. An operational theory for informationized warfare needs further work since the first battle is now more decisive in the overall course of the war.

- NCW's integrated weapons include inner space, outer space, information space, and psychological space weaponry (the latter category includes propaganda, deterrence, interference, and deception weapons).
- NCW enables real-time discovery and destruction, altering the traditional cycle of observe-orient-decide-act.
- NCW management must be on a systematic and network level with strict regulations and a legal basis.
- NCW should be incorporated into the Central Military Commission's strategies and policies immediately.
- In informationized warfare theory three nets must be supported—the sensor net, the weapons platform net, and the information net.

The book Study Guide for Information Operations Theory listed over 400 military terms. The book was chosen for inclusion in this volume because it is one of the few current sources and compendiums that list contemporary definitions. It has been over 20 years since Shen Weiguang first wrote about IW in 1985. Thus such a source does a few things: it allows one to track changes in definitions of old terms, it lists the meanings of new terminology, and it enables policy makers and analysts to view how the Chinese interpret and revise concepts and ideas that may have originated in other countries with their own “Chinese characteristics.”

In addition to the general definition of IW presented earlier, the Study Guide subdivided the Chinese concept of information warfare into several topic areas. These included: types of IW operations (offensive and defensive), IW sources (public information warfare and secret information warfare), layers of IW operations (strategic IW, combat IW, tactical IW), geographical IW areas (domestic IW, international IW), intelligence IW (political IW, economic IW, military IW, commercial IW, and diplomatic IW), and methods of IW acquisition (human IW, technical IW).

Another interesting Chinese emphasis in the Study Guide is on battlefield IW. The definition states that it revolves around “comprehensive countermeasures and combat conducted in the areas of warning, detection and reconnaissance, information transmission and processing, weapons control and guidance, operations command and control, camouflage, deception and interference, as well as around military stratagems.” Here again we see those terms that are often emphasized in Chinese military jargon when discussing IW: comprehensive, countermeasures, control, reconnaissance, and stratagems. With regard to the latter, the Chinese also defined what were deemed anti-information strategy technologies. Thus their writings show consistency over time with particular emphasis on a common set of IO terms of reference.

There is one term that is a Chinese equivalent of a US term that should not be overlooked. That term is informatized operations which the Study Guide states is the same or similar to integrated operations and NCW. The Chinese targeting order for informatized operations is somewhat new and includes psychological shock, material destruction, and physiological annihilation in that order. Again, the initial emphasis is on cognitive issues. The basic formula for informatized operations is the transformation of superiority in perception, intelligence, and decision making into operational actions. It is also important for informatized operations to prevent an enemy force from organized operations. The Study Guide defined informatized operations as

Two sides in a conflict relying to a high degree upon information, information systems, and informatized weapons and equipment. These operations involve information flow and systematic countermeasure actions undertaken in multiple spaces and realms such as on land, on the sea, in the air, in space, in the electromagnetic realm, in the realm of information, and in the realm of cognition.

Thus even this NCW equivalent concept also contains countermeasures and cognition. This Chinese emphasis must not be overlooked by US analysts since it appears in all of their key information-related terms. Informatized support operations include integrated reconnaissance systems, command and control systems, intelligent precision-strike systems, and operational-support and safeguard systems.

Other items of interest from the Study Guide that should be included in a concluding summary are the following:

- A list of the key elements of military power included computation, reconnaissance, simulation capabilities, communication capacities, and reliability. [Author's note: this type of military power does not appear to have a relation to CNP or comprehensive military power.]
- Information weapons have shrunk time and expanded the space in which they can operate. Strategy, combat, and tactics are so compressed that they almost coincide.
- The IO planning process includes: IO tasks (power to be used), information security and protection; important targets, a force's configuration and tasking, operational stages, the organization of command and coordination, and the time needed to complete preparations for information attacks and the ability to implement them.
- The basic thread in military thought about operational goals has been that one must lock onto an enemy's strength, consume his potential for war, and target the remnants of his will to fight with a final blow.
- Combat force is equal to the combination of energy and materials multiplied by information. Technology and strategy must be given equal weight, however, as cognitive systems are as important to attack as technological systems.
- Precision warfare includes precision information, precision control, precision movements, and precision strikes.
- Countermeasures to the concepts of time, space, and systems have brought about great changes to informatized war.
- The five major command and control elements are operational confidentiality, military deception, psychological warfare, electronic warfare, and firepower strikes.

The final book under review in the 2004-2006 timeframe was Warfare Strategy Theory. Also edited by Yao, the book continued the emphasis demonstrated in the Study Guide and in the Interpretation of Network Centric Warfare on cognition and strategy issues. With regard to features of informationized warfare, Yao listed its main features as follows:

- Informationized weapons are the dominant weapons on the battlefield in the form of platforms and ammunition.
- Information energy (reconnaissance, precision guidance, electronic warfare, etc.) is the principal capability unleashed on the battlefield in that it can control substance and capability.
- Informationized warfare is the principal form of war.
- The principle objectives of informationized war are the three major systems of battlefield cognition (surveillance, survey, navigation, etc.), battlefield communication (transmission of information), and battlefield guidance and control.
- Information superiority is the pinnacle of the battlefield struggle. Through information superiority other levels of dominance (airpower, naval space) are then possible.[\[709\]](#)

Final Thoughts

It was noted in the introduction to this work that the primary authors whose works were utilized were Shen Weiguang and Dai Qingmin. This obviously has created in the author and reader a bias of sorts toward their points of emphasis and description. In that regard, one point to address in this section is the extent to which these issues coincide with or deviate from other specialists views on IW/IO. A brief look through open source (publicly available) materials in the civilian and military sectors over the past three years demonstrates that the material falls into four categories: those items that coincide with Dai and Shen's views; those items that coincide with issues from Dragon Bytes; those items that are completely new; and those items that contradict either material in Dragon Bytes or in this volume.

A quick analysis of hundreds of reports from 2004-2006 shows the following general breakout of topics:

- Hackers/network warriors or reconnaissance units scanning the net for weaknesses
- The use of stratagems in conjunction with technology
- C4KISR discussions
- Network counterattacks or network weaknesses
- Optical fiber being laid in Xinjiang, Inner Mongolia, and under the ocean (by Verizon)
- Development of high-technology devices such as UAVs, simulation labs, chip-design labs, artillery munitions
- Thoughts on the war in Iraq
- Red versus blue confrontations in exercises designed to improve the informationization techniques of the force
- Space warfare, to include antisatellite warfare
- Psychological warfare techniques
- People's War in the information age
- Law as a weapon.

About three-fourths or more of these issues were discussed in either Decoding the Virtual Dragon or Dragon Bytes, so the coverage has stayed basically the same over the past eight years. New items included further explanations of IW/IO concepts or applications of concepts. Thus using Shen and Dai's description of IW/IO as a base for understanding Chinese concepts does not appear to lead the analyst too far astray.

The topic of countermeasures appeared often in all the definitions of important terms (IW, IO, informatized operations, etc.) and in explanations of how an inferior force fights a superior force. Dai, for his part, discussed countermeasures, specifying that multiple methods of flexible resistance (countermeasures) should be developed: net-shaped dispositions, jamming wireless reconnaissance equipment, carrying out reverse tracing and counterdestruction of enemy websites, paralyzing vital points, and developing situations using creativity. Over the past few years, the Chinese press carried articles on information countermeasures, Google Earth countermeasures, information construction countermeasures, electronic countermeasures, information gap and equipment countermeasures, and laser countermeasures, among other countermeasure issues. Most were discussed in important journals such as China Military Science.

A 1999 Chinese description of information countermeasures described Serbian countermeasures against coalition forces during the Kosovo conflict. The Chinese also discussed reports that the Russians had provided the Iraqis with frequency devices (countermeasures) that would offset the frequency control of cruise missiles or precision-guided missiles the coalition used in 2003 in Iraq. The Chinese most likely viewed these uses of technology as terrific examples of how to use countermeasures to offset high-technology equipment or how the inferior could offset the power of the superior. This emphasis on countermeasures should be expected to continue.

Is the term countermeasure simply an expression of the dialectic in action (measure, countermeasure) or does it have a deeper meaning? If it implies that an information-based conflict has such active offensive and defensive components that one must be thinking countermeasures from the start, then the Chinese definition has a leg up on the US simply for its focus on this issue. The only "counter" term present in the current US explanation of IO is counterintelligence. JP 3-13 does not even have counterpropaganda in its general discussion of IO (listing it only in an appendix at the back of the Joint Publication). This US reluctance to put more thought into "counter" concepts may come back to haunt it someday. For example, both the terms counterpropaganda and counterinfluence took on more significance in Iraq once combat with the insurgents began and the latter began using the Internet to spread its ideology.

The Chinese focus on cognition and beliefs as a major and growing component of its home grown IW/IO definitions indicates that it will be emphasizing countercognitive activities of some type to thwart anyone who tries to manipulate perceptions. There will be extensive internal and external efforts to shape or control domestic thinking as well as efforts to exploit holes in counterpropaganda efforts of foreign decision makers and foreign audiences. Cognitive activities are a way to win without fighting.

Another very interesting point to consider when examining IW/IO is the extensive knowledge that the Chinese have about our concepts and systems. When visiting a bookstore in downtown Beijing or Shanghai, for example, the military section (usually on the third or fourth

floor) contains Chinese translations of thirty or forty (perhaps more, depending on the size of the store) US military books. Several are translations of IW/IO books by US authors or authors from other nations. Translations of US field manuals are almost always available. The point to be made is that the Chinese do a much better job at “know the enemy and know yourself, and you’ll never fail in battle” than most nations. In the US, for example, much less is known about Chinese military theory and practice. A US military bookstore usually is limited to five Chinese titles: Art of War, Unrestricted War, Seven Military Classics, 36 Stratagems of War, and The Book of Changes. It would be a rare occurrence to find all of these titles in one place.

In addition to compiling an impressive list of Western military translations, the Chinese military has also assembled a host of agencies, centers, laboratories, universities, and other organizations involved in the study or application of IW, IO, or information security research. For example, the following were identified just in the research for this volume, which used a very limited number of sources:

- The National Information Security Support Management Agency
- Centers include: the National Information Security Center for Supervising Law Enforcement, the National Information Security Evaluation and Authentication Center, the National Information Security Crisis Handling Center, the National Information Security Legal Support Center, the National Information Security Education and Training Center, and the National Information Security Conflict Research Center
- Advisory Committee for the Informatization of the Military
- Information Operations Theoretical Research Office of the Operations Theory and Doctrine Research Department at the Department of Military Sciences
- Information Security University
- Information Confrontation Laboratory.

Finally, The Science of Military Strategy discussed Taiwan and implied what China’s strategy might be in an information-based environment. Strategic deterrence control was emphasized as one way to keep the Taiwan situation under control. Strategic deterrence control is the 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. Strategic operations and strategic deterrence are dialectically related, the book states. The former secures strategic objectives through direct engagement with the enemy on the battlefield while strategic deterrence’s objective is to contain the outbreak of war or limit its scope.^[710] One must possess a deterrent force, have the determination (which Peng and Yao state is the soul of deterrence) to use it, and make approaches urging the opponent to perceive the above-mentioned points, creating psychological pressure on an opponent.^[711] Today China’s deterrent force is based not just on missiles but increasingly on its information-based concepts and equipment, and it is integrating this technology into its overall strategy.

Further with regard to Taiwan, if strategic deterrence fails, then another potential course of action might be the following:

When the strategic offensive aim is seizure of the areas under the opposing side’s control,

the pattern of a naval and air vertical landing offensive will surely be adopted if in areas bordering on the sea or in large islands; and the multidirectional offensive pattern will be adopted if on land.[\[712\]](#)

One might say that there is concurrent emphasis on both deterrence and war-fighting in this regard since both of these options are clearly available to Chinese strategists. When political objectives are limited, and force utilization is more integrated and operational means are based on information, then more stress is placed on comprehensive strategic interests (CSI) than on war's destructive power.[\[713\]](#)

This concludes the decoding of the virtual dragon. The meaning of strategy and the extent of China's in-depth study and analysis of information-age issues should be apparent to the reader. Terms were laid bare and the application of Chinese characteristics to these terms was discussed. Hopefully the reader has gained a greater appreciation for the Chinese approach to IW/IO issues and how they may be fused with strategy. While these capabilities are looming larger every day, and more media pundits are highlighting the "Chinese threat" for us (as well they should, especially for the Chinese proclivity for overt reconnaissance) let us remember that the US still has more powerful capabilities. US policy makers must learn, however, to integrate strategy and technology as the Chinese have done, albeit in our case with "US characteristics," to remain aware and focused on the Chinese capability in this arena. Let us also hope that the full fury of either force is never used against one another and that US-Chinese-Taiwanese relations remain as peaceful tomorrow as they are today.

APPENDIX ONE: IW ARTICLES IN CHINA MILITARY SCIENCE: 2004-2006

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. 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 2004. 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, 2006
None

Number 5, 2006
None

Number 4, 2006
“Guiding Military Informationization Building with Scientific Development Concept,” Zhang Xunca, pp. 20-23.
“Basic Laws of Operations of Military Information Command Systems,” Wang Liyong and Huang Tao, pp. 97-102.
“Strengthening Studies on Combat System Confrontations of Naval Campaigns,” unclear from a list of names who authored this article, pp. 141-142.
“Issues to be Stressed in the Informationization Building of our Military from the Transformation of the US Military,” unclear from a list of names who authored this article, pp. 147-149.

Number 3, 2006
“Guide the Creative Development in Military Training under the Information Conditions with Scientific Development Concept,” Wang Jianmin, pp. 1-7.
“Network Warfare and Complex Networks,” Li Deyi, Wang Xinzheng, and He Gangfeng, pp. 111-119.
“The Development of Warfighting Platforms and their Impact on the Military,” Li Daguang and Liu Yanjun, pp. 120-130.

Number 2, 2006
“Fully Improving Informationized Operational Capabilities of the Military under the Guidance of a Scientific Development Concept,” Zheng Zhanping, pp. 11-16.
“Views on the Development of an IPV6 System for Military Information Networks,” Chen Peng,

Gu Xiaoming, and Dai Hao, pp. 124-130.

Number 1, 2006

“On Creating Military Theories under Information Conditions,” Sun Haicheng, Lin Huasheng, and Liang Huan, pp. 84-88.

“Development of CPLA Psychological Warfare Thinking in War Times,” Jiang Yibin, Wu Juncang, pp. 109-114.

Number 6, 2005

“General Reflections on Integrated Training under Informational Conditions,” Zhunag Xunca and Qiu Guijin, pp. 99-104.

Number 5, 2005

None

Number 4, 2005

“On the New Requirements of Information Warfare on Combat Spirits,” Ma Gensheng and Wong Yi, pp. 80-83.

“An Analysis of Combat Spirits of Military Talents under Information Conditions,” Shen Guoquan and Zhu Fangqin, pp. 84-89.

“Adhering to Putting People in the First Place in Promoting Information Construction,” Zhang Yonggang, pp. 108-115.

“Concept and Characteristics of Strategic Psychological Warfare,” Jiang Jie and Wu Juncang, pp. 126-129.

“A Study of the Operational Mechanism of Psychological Warfare,” Hao Weixue and He Lingfeng, pp. 130-133.

“Characteristics and Trends of US Strategic Psychological Warfare,” Wang Lianshui, Zhou Jianxin, and Dong Jianmin, pp. 144-150.

Number 3, 2005

This issue had an entire section devoted to psychological operations titled “Theoretical Study of Strategic Psychological Warfare.” The first five articles below are in that section.

“On Cultural Identification and National Reunification,” Yang Yuling, pp. 57-63.

“Modern Cultural Diffusion and National Security,” Wang Shudao, pp. 64-69.

“Media Warfare in Informationalized Conditions,” Cui Changfa and Tang Fuquan, pp. 70-76.

“Important Issues Concerning Strategic Psychological Warfare under Informationalized Conditions,” Chang Yan’e and Ou Lishou, pp. 77-83.

“Characteristics of Psychological Strategy in US Strategic Thinking,” Xu Jia, pp. 84-87.

“Issues of the Study of War Complexity under Informationalized Conditions,” Shen Shoulin, Zhao Shuchun, and Zhang Guoning, pp. 118-125.

Number 2, 2005

This issue has the entire first section devoted to “Strategic Thinking of Military Information Construction.”

“Scientific Guidance to Building Informationalized Armed Forces,” Yang Yeli, pp. 2-11.

“Guiding Military Information Construction with the Concept of Scientific Development,” Wang Fa’an, pp. 12-17.
“Strategic Thinking and Countermeasures in Military Information Construction,” Liu Jixian, pp. 18-25.
“Deliberation on Military Information Development Strategy,” Chang Wen, pp. 26-30.
“Discussion on Status Quo and Countermeasures of Military Information Construction,” Zheng Qin, pp. 31-38.
“On Technological Organization and Leadership in Military Information Construction,” Sun Haicheng, Ji Shidong, and Mi Guoqing, pp. 39-46.
“Military Strategic System of the Information Era,” Zhang Feng, Liu Zengliang, and Lu Dehong, pp. 90-99.
“On Digital Logistical Management in Modern Armed Forces,” Wang Qihua, pp. 100-106.

Number 1, 2005

“An Analysis of the Features of Information Warfare,” Wang Mingliang, pp. 20-26.
“Differentiation of Command Automation and the Prospect of Informationalization of the Armed Forces,” Chang Guocen, pp. 72-78.
“Considerations of Improving Mobilization in Regional Information Warfare,” Chen Ying, pp. 91-97.
“Summary of Symposium on the Informationalization of the Army Political Work Theory and Practice,” Tan Zhixing, Zhang Yu, and Liu Yongdan, pp. 148-151.
“Summary of Symposium on the Study and Application of Sun Tzu’s Art of War in the Information Age,” Xue Guoan and Chen Xiangling, pp. 152-156.

Number 6, 2004

“Sun Tzu’s ‘Winning Conception’ and Air-Space Power in the Information Age,” Zhang Zhiping, pp. 35-39.
“Understanding the Duty of Army Propaganda and Cultural Work and Taking the Lead in Building Advanced Culture,” Wu Changde, pp. 60-67.
“Trends in the Development of Operations Command under Informationized Conditions,” Li Zhangrui, Song Guangshou, Liu Kui, and Deng Zhao, pp. 90-96.

Number 5, 2004

This issue has an entire section devoted to information warfare titled “Theoretical Study of Information Warfare.” The six articles below are in that section.

“Decision on Further Promoting the Development of the Philosophy and Social Sciences Doctrine of the Guidance of Information Operations,” Che Xianming and Wang Wei, pp. 9-16.
“Basic Features of Information Operations,” Li Yinnian, Sun Qiangyin, and Sun Jianjun, pp. 17-24.
“On Information-based Warfare,” Zhang Zhanjun, pp. 25-36.
“On Integrated Joint Operations Based on the Military Information Network,” Cui Yafu, pp. 37-42.
“Views of Creation in Information Operations Command,” Li Chunli, Chen Yilai, Jin Guomin, and Wang Yunlei, pp. 43-49.
“Information Warfare and Changes in the Essentials in Military Thinking,” Yan Gaohong, pp. 50-55.

Number 4, 2004

This issue has an entire section devoted to psychological operations titled “Study of the Theory of Strategic Psychological Warfare.”

“A Study of the Theory of Marxist Strategic Psychological Warfare,” Han Qiufeng, pp. 34-41.

“On the Basic Features of Strategic Psychological Warfare,” Wang Baoshan and Li Peng, pp. 42-47.

“Theoretical Consideration of Strategic Psychological Warfare,” Zhu Huaqing and Yi Dazhang, pp. 48-56.

“Competition and the Contest of National Culture,” Yan Xiaofeng, pp. 57-68.

“On Religious Psychological Factors in National Conflicts in the Contemporary World,” Wang Zhiping, pp. 64-68.

“Developing Trends of Psychological Warfare in Grand Strategy,” Yao Zhenqing and Meng Yan, pp. 69-74.

“The Direct Manifestation of the Operational Role of Political Work—On Media Warfare, Psychological Warfare, and Law Warfare,” Lin Ronglin, pp. 91-95.

“Characteristics of Information Mobilization,” Sun Haicheng and Zhang Zhen, pp. 101-105.

Number 3, 2004

“Creatively Advancing the Science of Information Operations with PLA Characteristics,” Xu Xiaoyan, pp. 37-43.

“An Outline of the Theory of a System of Systems,” Zhao Cunru, pp. 44-49.

“Views on Pushing Forward the Informationization of the PLA,” Liu Jianguo, pp. 97-101.

“Dialectical Understanding of the Issues of Defeating a Powerful Enemy with a Weak Force in High-Tech War,” Deng Feng, pp. 107-111.

Number 2, 2004

“On Jiang Zemin’s Theory of Army Informationization,” Niu Li, pp. 30-37.

“Details of the Psychology of Oriental Strategies,” Wang Zhenxing, Zhou Jianxin, and Yi Hui, pp. 120-130.

“Study of Protective Engineering under the Conditions of Informationized War,” Zheng Yingren and Li Xiudi, pp. 142-147.

“Realizing the Transformation of Military Form from Mechanization to Informationization,” Xia Zhengnan, pp. 148-156.

Number 1, 2004

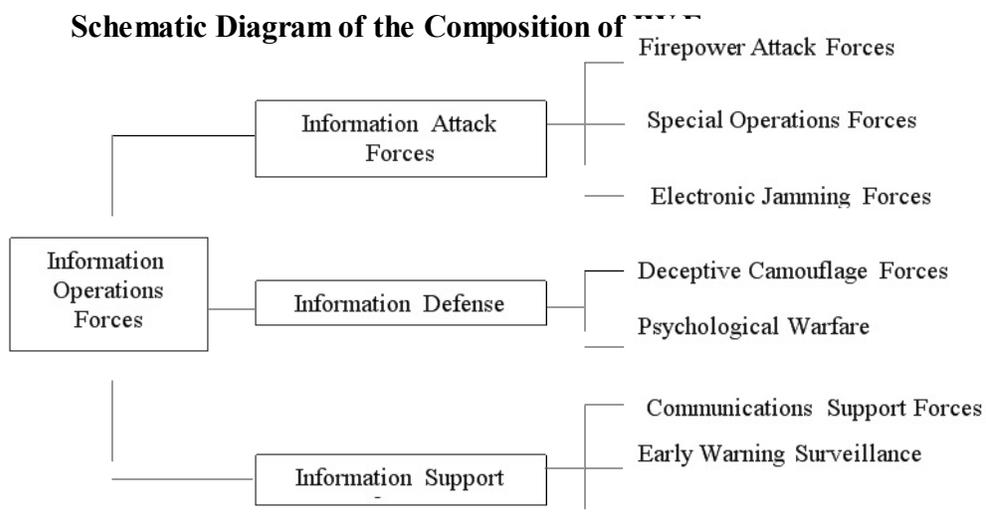
None

APPENDIX TWO: IW DEFINITIONS IN THE CHINESE MILITARY ENCYCLOPEDIA [\[714\]](#)

In the summer of 2004, the book Dragon Bytes was published. The publication described Chinese information warfare (IW) developments from 1999-2003. The present book covers Chinese IW developments from 2004-2006. However, the author obtained several important IW related items from the 1999-2003 timeframe only after the publication of Dragon Bytes. One of these items was the Chinese Military Encyclopedia.

The encyclopedia contains a more detailed, and perhaps more authoritative, definition of information warfare, information warfare technology, and operations research and analysis of information warfare than those obtained from journals. These three entries are listed below in this appendix in their entirety with topic headings in English and Chinese. These are the most “official” or authoritative definitions of Chinese IW obtained to date, to include the post-2003 timeframe.

Information Warfare [xinxizhan]—Operations carried out to seize and maintain information supremacy (FBIS translators consulted for this definition defined the term supremacy as “control”). According to time, it can be divided into peacetime information warfare and wartime information warfare. Peacetime information warfare refers to commonly conducted hostile, two-party information confrontation in periods of peace in areas such as politics, economics, science and technology, foreign relations, culture, and military affairs.



Wartime information warfare refers to hostile, two-party information warfare carried out in periods of war. It includes using many kinds of measures to attack the enemy’s information and information systems; to damage or sever the enemy’s flow of information; and to influence,

weaken, or destroy the enemy's information operations capabilities while safeguarding the information operations capabilities of one's own side. Information warfare includes two mutually connected aspects, and those are information attack and information defense. Information attack is fully utilizing various information technology measures to influence and weaken the adversary's information operations capabilities via methods such as information blockade, information deception, information interference, information contamination, and information destruction. Information defense uses information secrecy, information safeguards, and other methods to safeguard the information, information systems, and information operations capabilities of one's own side from the influence of enemy information attack. Information warfare is various actions to expropriate, utilize, damage, or destroy the enemy's information, information systems, and information operations capabilities while safeguarding and fully utilizing the information, information systems, and information operations capabilities of one's own side. Its goals are to capture and maintain information dominance; to fully control the right of access to, the right of control of, and the right of use of information; and thus gain the initiative and the advantage in war.

Brief History

Information warfare is a new form of operations that emerged in the transition from the industrial age to the information age following the informationization of society and military informationization. Since the 1970s, following the swift development of information technology and the unceasing enhancement of the informationization of society, information technology has become an important basis for the development of society, the rapid rise of the economy, the progress of science and technology, and the power and prosperity of the nation. Information has already become an important resource for the growth of society. At the same time, informationization has also become an important part of armed forces modernization building. Gaining information dominance and controlling information supremacy have become crucial links in winning war dominance. Under these circumstances, hostile, two-party confrontations and contentions in the field of information are becoming more and more intense. All kinds of specialized information weapons are continually coming forth, and traditional information confrontation is gradually evolving into a new form of operations. American T. Rona was the first to bring up the idea of information warfare. In 1976, he pointed out, "Information warfare is combat between decision making systems." (US Military Intelligence magazine, January-March 1997, D. Diersi, "Content, Characteristics, and Influence of Information Warfare") [Note: The name transliterated above may be Diels, Deers, or another similar sounding name.] In the mid-1980s, in keeping with the reality of the increasingly fierce information confrontations in all operational fields, the US Air Force and Navy formally used information warfare concepts. After the Gulf War, many of the countries in the world progressively followed information warfare with interest and attached importance to it. They used information warfare as an important measure to realize their military strategies, and they launched extensive research and practice. In 1992, the US Department of Defense issued secret orders about enhancing information warfare research, asking all services and arms to launch extensive theoretical research and preparations for information warfare. In January 1995, the US Department of Defense set up an information warfare implementation committee, and it established the "National Defense Information Bureau." The Army, Navy, and Air Force also each set up "information warfare centers" that were specifically responsible for researching and directing information warfare. Since 1996, the US military has issued a series of policies, rules, laws, regulations, and doctrine, including "Naval Operations Department Instruction 3430.26: Implementing Instruction for Information Warfare and Command

and Control Warfare;” the Air Force’s “Cornerstones of Information Warfare;” Chairman of the Joint Chiefs of Staff regulations “Chairman of the Joint Chiefs of Staff Instruction 3210.01: Joint Information Warfare Policy,” “Joint Doctrine for Command and Control Warfare,” “Chairman of the Joint Chiefs of Staff Instruction 6510.01A: Defensive Information Warfare Implementation,” “Joint Vision 2010,” and “Joint Information Warfare;” the Army’s “Field Manual 100-6: Information Operations;” the Defense Science Board’s “Defensive Information Warfare Strategy,” “FM 100-6: Information Warfare,” etc., to regulate military and civilian information warfare activities. At the same time, the US also put as much as one hundred billion US dollars toward research and development for all kinds of new information warfare weapons. In order to effectively carry out preparations for information warfare, the US conducted a large number of information warfare simulation exercises and increased the information confrontation content at all levels and in all kinds of military exercises. In 1995 and 1996, RAND Corporation held two large scale information warfare simulation exercises. Russia established the National Information Policy Commission, subordinate to the president, and it set about organizing corresponding functional organizations, enhanced the technical and personnel training required for information warfare, emphasized developing key information warfare technologies and weapons, and increased technology imports from abroad. Britain, France, Germany, Japan, and India also established related organizations to direct information warfare and enhanced direction and coordination for researching and preparing for information warfare. From this point, information warfare has already been widely accepted in world military circles as a kind of new form of operations in modern war. At the same time they enhanced research into information warfare theory, all the principal countries in the world also intensified technological and tactical preparations for information warfare. They organized information warfare units and gradually used some information warfare measures and methods in real war during the limited wars of the 1990s. The Gulf War in 1991 and the Kosovo War in 1999 were important test beds for information warfare, and they showed that information warfare had in all respects moved from theoretical research toward utilization in real war.

In the 1990s, the Chinese People’s Liberation Army had fully developed theoretical research into information warfare, and in 1990, it published the book Information Warfare, the earliest monograph to study information warfare. Following this, a large number of theoretical research achievements were published in succession, including “The Science of Information Operations Command and Control,” “The Science of Information Operations Technology,” “An Outline of Information Operations,” and “An Introduction to Information Operations.” At the same time, information warfare technology attained rapid growth, and the work of training combined arms commanders in information warfare abilities made significant progress. Information warfare had already permeated joint operations exercises.

Characteristics

Information warfare is a form of operations in which information plays the dominant role. It has the following prominent characteristics. (1) Intensity in the Fight for Information Supremacy. In modern and future wars, information has already become a key factor in gaining the upper hand. Forming and bringing into play the combat effectiveness of an armed force primarily depends on obtaining, processing, transmitting, controlling, and using information. Because of this, in joint operations, the struggle for information supremacy will be unusually incisive and intense, and it will run through the entire course of war. (2) Immediacy in Reaching Operational Objectives.

Information warfare has enemy information, information systems, and information operations capabilities as its immediate targets. It really attacks the enemy's command decision making systems or support systems, and once it damages or destroys these targets, it can directly shake the enemy's decision making intentions and operational determination, thereby immediately attaining the operational objective. (3) Integration of Operational Actions. Information warfare is highly integrated warfare. It is mutually coordinated and highly integrated with land, sea, air, and space operations, and operations in other spheres. It is an entire information confrontation and struggle that unfolds simultaneously across the battlefield space. (4) Indistinct Wartime and Peacetime Boundaries. Not only can information warfare attack the enemy's military information systems to disintegrate its military information capabilities, it can also attack the enemy's civilian information systems and national information infrastructure to damage or destroy its entire information operations capability. Not only can this kind of attack occur during wartime, it can even occur in peacetime, further blurring the boundaries between wartime and peacetime. (5) Highly Efficient Attack Results. By directly attacking the enemy's information, information systems, and information operations capabilities, information warfare can damage or destroy its entire military and socio-economic systems, which are supported by information and information systems affecting and weakening its overall national strength.

Forms

Information warfare includes many forms, such as command and control warfare, intelligence warfare, electronic warfare, psychological warfare, network warfare. Command and control warfare is the core of information warfare. It is essentially using methods such as physical destruction and electronic attack to interfere with, damage, and even destroy the enemy's command and control system, weakening or damaging the enemy's command and control capabilities while protecting one's own command and control systems from the effects of similar enemy actions, ultimately seizing information supremacy and controlling battlefield initiative. The goal of intelligence warfare is to use various information surveillance measures to capture information, allowing one's own commanders to receive timely and accurate intelligence information while using various measures and means to leave enemy commanders no way to obtain required intelligence information. Electronic warfare is an electro-magnetic fight to weaken or damage the usefulness of the enemy's electronic equipment and ensure that one's own electronic equipment operates normally. It includes a series of actions to prevent the enemy from using the electro-magnetic spectrum while ensuring that one's own side can make full use of the electro-magnetic spectrum. 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. This is a new development of psychological operations under modern high-technology conditions. Its goal is to psychologically attack the enemy, achieving victory without fighting, or fighting and winning. Network warfare is operational activities to interfere with, damage, destroy, or control the enemy's information network by using measures such as damaging computer software, attacking it with viruses, and destroying its hardware. In this way network warfare influences or damages the military systems and national information infrastructure which are based on information networks while protecting one's own information network-based military systems and national information infrastructure from the effects of similar enemy actions. In information warfare, the main operational forms above are interrelated and intertwined.

Looking Ahead

Information warfare will rapidly develop in the following respects. (1) Improving Information Warfare Theory. Based on the results of research into current information warfare, further exploration of the characteristics and laws of information warfare and study of the relationships between information warfare and other forms of warfare will take shape as informationized warfare theory. (2) Developing Information Warfare Technology. IW will utilize the newest achievements in modern information technology, research and development of new information warfare technologies, especially high-efficiency information warfare weapons. (3) Innovation of Information Warfare Methods of Operation. This includes research and innovation under different conditions to realize effective tactics and methods for information warfare. (4) Strengthening and Developing Information Warfare Units. Based on informationization of the armed forces and digitization of the battlefield, they will organize special information warfare units and fendui to specifically engage in information attack and defense to make preparations for information warfare. Along with the ever-increasing perfection of information warfare tactics and methods of operation, information warfare will play an increasingly important role in future war. [\[715\]](#)

Information Warfare Technology [xinxizhan jishu]—Technology used to seize information dominance in order to influence the opponent's information, information systems, and basic information structure and protect one's own in hostile, two-party confrontations conducted in the realm of information. Information warfare technology is an important measure for conducting information warfare.

Information warfare technology involves all fields of information technology, including information gathering, information processing, information transmission, information management, and information application. According to operational models for information warfare, information warfare technology can be classified as information warfare attack technologies, information warfare defense technologies, and information warfare support technologies.

Information warfare attack technologies include the following. (1) Information Deception Technology. That is, technology that transmits false information to the enemy's information systems, various sensors, and media. This includes various deception and camouflage technologies and stealth technology, and it causes the enemy to make erroneous decisions when the information is received. (2) Electronic Attack Technology. That is, technology that uses electronic jamming, deception, or direction-finding weapons to weaken or destroy the enemy's ability to make use of the electro-magnetic spectrum. (3) Computer Network Attack Technology. This is attack technology for computers and computer network hardware and software. "Hackers," computer virus weapons, "worm" programs, "trojan horse" programs, logic bombs, system traps, and "hardware tricks" are frequently used attack technologies. They make computer hardware and software ineffective, or they delete, append, replace, and steal data. (4) Material Destruction Technology. That is, using precision guidance weapons and other weapons to carry out hard kills against enemy information systems and their power and supply support systems. Material destruction technology includes viruses that attack hardware, antiradiation weapons, nuclear electro-magnetic pulses, microwave weapons, laser weapons, etc. (5) Psychological Warfare Attack Technology. This is information processing technology that is implemented to psychologically influence the enemy using television, radio broadcasts, computer networks, and other media.

Information warfare defense technologies include the following. (1) Information Encryption Technology. This mainly refers to using low probability of intercept technology for one's own information. (2) Antimilitary Deception Technology. This mainly refers to identifying fake facilities in the enemy's deployment and using identification friend-or-foe technology to identify false enemy information. (3) Electronic Defense Technology. This includes electronic jamming countermeasures, electro-magnetic reinforcement, frequency allocation, information secrecy, antistealth, and other technologies. (4) Computer Network and Software Security Defense Technology. This mainly refers to computer security technology including isolation and screening, access control, cryptographic techniques, nonstandard design, system monitoring, integrated management, and other technologies. (5) Material Destruction Countermeasures and Psychological Warfare Technology Countermeasures.

Information warfare support technologies mainly refer to technologies for stealing, intercepting, and using the enemy's information. These include information reconnaissance technology, information processing and cracking technology, etc. It is the basis and prerequisite for conducting information attack and information defense.

Comprehensive electronic information systems are main battle weapons that seize information dominance. In information operations, they perform many kinds of operational functions, including command, control, communications, intelligence, monitoring, reconnaissance, navigation, information attack and defense, etc.

Electronic warfare technology is an important component of information warfare technology. Its earliest rudiments were in the early 20th century. Wireless communications countermeasures emerged during the First World War, and following that, radar countermeasure, opto-electric countermeasure, and hydro-acoustic countermeasure technologies emerged. Since the 1970s, because of the extensive use of information technology, information has become a key element of systems, and information warfare has become a new form of operations. Information warfare technology has attained rapid growth. The main development trends of information warfare technology are: developing information warfare support measures (ISM) [sic], information warfare command and control systems, computer security and attack technologies, and researching new concept weapons such as laser weapons, microwave weapons, and nanometric weapons. [716]

Operations Research and Analysis of Information Warfare [xinxizhan yunchou fenxi]—This theory includes a quantitative analysis of information warfare issues and selects the optimal plans, methods, and actions for their use. This mainly includes operations research and analysis of electronic confrontation and operations research and analysis of computer network confrontation. The two primary functions of operations research and analysis of information warfare are planning and preparing the optimal disposition and the best plans for military action to acquire the biggest operationally effective information weapons system; and analyzing, evaluating, and calculating the operational efficacy of information warfare weapons systems and plans for military action. The goal is to provide theoretical guidance and a quantitative basis for supplemental decision making in information warfare.

Forms and Development

Operations research and analysis of information warfare is gradually developing along with the continually deepening understanding of information warfare. During the periods of the First World War and the Second World War, the technology of using radio to disseminate information gradually matured. The main forms of information warfare, which was in its rudimentary period, were using codes and breaking codes, and specific examples of using operations research and analysis of information warfare were becoming more common. For example, the US military's successful breaking of the Japanese military's code directly led to the shooting down of the aircraft in which the Japanese military's Admiral Isoroku Yamamoto was riding. In the wars of the Middle East and the Vietnam War in the 1960s and 1970s, along with massive use of missiles and other informationized weapons and the consequential development of operations research decision making and efficacy analysis, operations research and analysis of information warfare began in the modern sense. In the 1980s, high-technology measures were used for capturing, transmitting, processing, and storing operational information, and the theory and practice levels of operations research and analysis of information warfare raised a great degree. During Israel's 1982 invasion of Lebanon, the Israeli military used electronic confrontation and reconnaissance measures to successfully entice Syria into revealing the technical parameters of its radar in Bekaa Valley. Then it used highly directional radar countermeasures to successfully attack and destroy the Syrian military's air defense missile bases. After the mid-1980s, following the rapid development of computer network technology, operations research and analysis of network attack and network defense as another important part of operations research and analysis of information warfare effectively penetrated and disrupted the enemy's information systems and protected friendly information systems, becoming an important subject in operations research and analysis of information warfare. During the Gulf War in the early 1990s, the multinational force headed by the US used the theory and methods of operations research and analysis of information warfare throughout the war which basically assured the centralized coordination of air attacks, the precision of airborne attacks, and the accurate evaluation of damage results. During the Kosovo War at the end of the 1990s, the North Atlantic Treaty Organization, with the support of its enormous information network, actively used operations research and analysis of information warfare methods to plan airborne attacks against the Federal Republic of Yugoslavia. The Federal Republic of Yugoslavia also used operations research and analysis of information warfare methods such as camouflage and deception to avoid a number of losses. During this war organized network attack activities also emerged, making computer network confrontation and its operations research and analysis become an organic part of information warfare for the first time. The development of operations research and analysis of information warfare entered into a relatively mature phase.

Research Content and Methods

Research content of operations research and planning of information warfare includes: optimal disposition of information warfare weapons systems, selection of the best plan for information warfare actions, information warfare countermeasures, optimal design and operation of information warfare equipment, evaluation and analytical calculation of the effectiveness of information warfare operations and equipment. Frequently used methods are mathematical planning, game theory, queuing theory, computer operations simulation, and virtual computer confrontation testing. Mathematical planning theory can be used to help come up with the best plan

for information warfare actions and for problems in information warfare concerning allocating weapons, selecting positions, organizing operations, and arranging personnel. Problems with information warfare countermeasures can be analyzed using game theory methods but with only a little pure strategy and with a lot of mixed strategy. Static state optimal design and operation of information warfare equipment can be analyzed using queuing theory methods, and various queuing models can be set up according to the characteristics of the input processes, queuing rules, and service systems. Moreover, calculating and comparing the service probability and the nonservice probability of information warfare equipment provides a basis for normal use of information warfare equipment. Simulated network confrontation testing is a special technical measure for resolving operations research and analysis issues for computer network confrontation based on specific types of computer network confrontation installations and software. It establishes a generalized mathematical model of network confrontation operations environments, confrontation actions, and confrontation processes by setting up a virtual network confrontation testing environment and imitating an opponent's network operating systems, database systems, and encryption mechanisms. By numerous attack tests against the target network and counting the capture frequency, it can assess the operational efficacy of network attack technology and equipment, calculate the results of tactics and plans, compare the strengths and weaknesses of different scenarios, and debug network attack software. It can provide decisive or quantitative references to make decisions for attacking the enemy's networks.

More and more, efficiency assessments and analyses of information warfare actions and equipment is beginning to use computer operations simulations. They can establish digital models of information operations environments, operational actions, and operational procedures and equipment based on the scope of the information warfare actions and the specific equipment types. It can evaluate the operational efficacy of the information actions and equipment, calculate the results of tactics and plans, compare the strengths and weaknesses of different scenarios, and revise the tactical and technical parameters of equipment by numerous computer simulation tests and processing statistics. Based on the size of the scope involved in the model, information warfare operations simulations are classified into four types: one-on-one confrontation, which is confrontation of an individual piece of electronic equipment against another individual piece of electronic equipment; many-on-many confrontation, which is confrontation of many pieces of electronic equipment against many pieces of electronic equipment; system-on-system confrontation, which is confrontation between both sides' operational information systems; setup-on-setup confrontation, which is confrontation between both sides' operational information setups.

Development Trends

Along with the continual deepening of theoretical research into information warfare and the progressive perfection of technical measures, information warfare is developing toward being more intelligent and being made into platforms. This places even higher demands on operations research and analysis of information operations. Along with the continual development and perfection of information warfare theory and practice, operations research and analysis of information warfare will increasingly make use of computer simulation decision making activities to reduce the subjective nature of researching to make decisions.[\[717\]](#)

APPENDIX THREE: SUN TZU ART OF WAR CONFERENCES AND IW SUBJECTS[\[718\]](#)

In November 2004, China held its 6th International Symposium on Sun Tzu's Art of War. In addition to hundreds of Chinese military and civilian officials, guests from Taiwan, France, India, Russia, and the US attended. Approximately 127 papers were listed in the program. Chinese speakers accounted for 109 of the presentations while five papers were from Taiwan, five from Hong Kong, and the remaining eight papers were from other foreign guests. Not all of the people listed in the program were able to be present, but abstracts of their papers were provided.

Chinese speakers stressed several themes. One was that US successes in Iraq were due to a reliance on Sun Tzu's theories more than those of Clausewitz. Five papers discussed some aspect of the war in Iraq. Another theme was that Sun Tzu's theories are applicable to the information age. Therefore the wisdom of Sun Tzu must still be followed and not discarded. Finally, several of the presentations discussed strategic culture or one of its aspects.

The Chinese presentations that addressed Sun Tzu's impact on psychological and information operations, the focus of this book, were few in number and are listed below.

1. "A Few Issues Concerning Sun Tzu's Art of War and Strategic Psychological Warfare" by Hao Yinglu and Zhao Xiaomin.
2. "The Basis for the Psychological Warfare Planning of Sun Tzu" by Zhou Min
3. "Enhancing the Psychological Warfare Capability against Taiwan by Learning from Sun Tzu's Military Thoughts" by Yu Jiang and Xiong Yuiang
4. "Sun Tzu's Strategic Thought and Its Inspiration for Informationized Warfare" by Chai Yuqiu
5. "Sun Tzu's Thoughts on War and Reflections on Informationized Warfare" by Jiang Lei
6. "Sun Tzu's Thought of 'Subduing' and Aerospace Power of the Information Era" by Zhang Zhiping
7. "Sun Tzu's Idea of 'Deception' and Information War" by Wang Huqiang
8. "Sun Tzu's Ideas on Psychological Warfare and their Direction in Modern Psychological Warfare" by Ai Songru

Three articles, those by Yu Jiang and Xiong Yuiang, Zhang Zhiping, and Wang Huqiang, were not available as handouts in complete length. However, abstracts of their presentations were available and will be noted in the discussion below.

A Few Issues Concerning Sun Tzu's Art of War and Strategic Psychological Warfare[\[719\]](#)

One key lesson that Chinese military authors have frequently cited over the past two years

regarding Iraq is that psychological warfare (PSYWAR) now has strategic significance. Authors Hao Yinglu and Zhao Xiaomin of the Xian Political Academy continued this discussion at the Sun Tzu conference. They defined strategic psychological warfare (SPW) as

a competition, a comparison, and a match of the overall forces of the enemy and friendly sides. It is a form of international political struggle that is related to the rise and fall of a nation and the waxing and waning of its strengths and vulnerabilities...it is a strategy for persuasion that uses psychological attack as the primary measure and confrontation as the main contradiction.

SPW reflects the interests and requirements of a country and their political intentions according to Hao and Zhao. On the military level, SPW reflects political objectives, making war an extension of politics and SPW (and not just politics as Clausewitz noted). This is a striking statement in its own right, and it demonstrates the focus the Chinese have placed on SPW.

The authors restated several of Sun Tzu's sayings, and they gave the clear impression that warfare is an offensive oriented task. One must contend for the initiative and control it. Hao and Zhao also stressed the offensive necessity to "impose one's will on the enemy but not allow the enemy's will to be imposed on oneself." SPW cannot have an inactive defense or be purely defensive. The focus must be on attack in order to gain the initiative. It must also utilize excellent forecasting and deep insight, and control preemptive opportunities. SPW must flexibly lay down strategic policies and plans for psychological war and use them to counteract an enemy's high-level decision makers.

The authors stated that one must be good at "temple calculations" or planning as well. Moral law, heaven, earth, the commander, and method and discipline govern temple calculations. Here one must ask of a confrontation

Which of the two sovereigns is imbued with Moral Law? Which of the two generals has the most ability? With whom lie the advantages derived from heaven and earth? On which side is discipline most rigorously enforced? Which army is stronger? On which side are officers and men more highly trained? In which army is there the greater constancy both in reward and punishment?

To properly utilize SPW requires an understanding of the objective and subjective conditions of the enemy and friendly sides. Calculations based on this understanding ensure that strategic decisions are properly made, the authors contend. These decisions must take into consideration the strategic focal points, orientation, and missions of a country. It is necessary to combine all of one's strategic resources and to employ direct and indirect uses of SPW in combination. SPW requires military, technological, economic, and information superiority. Further,

Superiority in ideological culture can have an effect on the enemy's ideological concepts, ideology, and cultural traditions; it can subdue and control the mind of the enemy; it can create changes in the relationship of the authorities of the two sides.

Any psychological struggle must be backed by substantial military strength. This has also

been a longstanding proposition of the PLA, much like the focus on SPW. PSYWAR and power are related because together they intimidate.

The Basis for the Psychological Warfare Planning of Sun Tzu[720]

Author Zhou Min, from the Sun Tzu Art of War Application Consultation Center, discussed the values, methods, forms, and thoughts on PSYWAR in his dissertation. To Zhou, PSYWAR was about penetrating the enemy soldier's mind or that of the command decision maker with deception. He also wrote briefly on the theory of morale and associated it with times to attack and the condition of a soldier's hypothalamus gland (clearly, this is a surprise to most Western specialists!).

Zhou noted that planning for deception depends on correctly using the "form of units," suggestion, and what is known as "breakthrough" in psychological lines of defense. Unit "form" means moving units around, camouflaging them, and reducing or increasing their numbers. These various forms put suggestions into the heads of opponents. Suggestions capitalize on veiled language or information as well as indirect action to have an effect on the psychological behavior of people. Suggestion based on form then produces breakthroughs in the ability to control the logic, morale, and lines of defense of the enemy's decision makers. Morale is a type of combat strength of an enemy, an expression of the collective spirit and collective will of military personnel. It is best to attack morale in the evening. Scientifically, this works because when under stress the feedback control loop between the hypothalamus, the pituitary glands, and hormones in the brains of military personnel can fall out of balance due to excessive releases by the hypothalamus, lowering moods and excitement.

Today psychological pressure on commanders and national decision makers is greater than at any time in the past. Psychological warfare operations include strategic deception, forms of electronic information, propaganda, and shock and awe types of information. These PSYWAR operations are designed to attack lines of defense and produce faults in policymaking and induce compromise in policy makers.

Of interest is Zhou's formulation of what he terms "operational forms of PSYWAR." These forms of psychological war now include propaganda PSYWAR, deterrence PSYWAR, conscious PSYWAR, ideological PSYWAR, and network PSYWAR, among others. Unfortunately he did not go into depth and explain any of these forms. The ultimate goal is to gain psychological supremacy and change the cultural values of PSYWAR targets.

In addressing US armed forces in particular, Zhou noted that they operate on five principles. These are initiative, depth, agility, coordination, and multiple abilities. The US military aims to destroy forces materially and "what is even more important" to create intense psychological shock and awe in the enemy's mind to destroy cohesion and the will to fight.

Sun Tzu's Ideas on Psychological Warfare and Their Direction in Modern Psychological Warfare[721]

Author Ai Songru of the Shenyang Military Region offered a longer, more detailed perspective on psychological operations. His remarks covered the use of PSYWAR in Iraq, the abundance of new PSYWAR techniques available, and a discussion of how China must prepare itself to exploit the wisdom of Sun Tzu. He also focused attention on the elevation of PSYWAR to a position of strategic prominence affecting political, military, and diplomatic struggles.

Ai noted that he studied the use of PSYWAR in Kosovo, Chechnya, Afghanistan, and Iraq and paid attention to the psychology of both sides. He discovered problems for coalition forces that included coordinating PSYWAR strategy, measures, and support before, during, and after these wars. Problems arose in Ai's opinion because people did not "completely decipher Sun Tzu's ideas on PSYWAR or use PSYWAR as it should have been applied." He felt that Eastern wisdom and Sun Tzu's ideas on PSYWAR are required if the world is ever to experience peace and growth.

Ai stated that the widespread use of modern broadcast technology, network technology, stealth technology, virtual reality technology, three-dimensional imaging technology, composite audio-visual information technology, and so on has made PSYWAR measures more abundant. This allows for PSYWAR to be used during the entire course of a war. In Iraq, Ai believes the US made PSYWAR strategy the basic strategy of the war. PSYWAR improved the result of operations and accelerated the progress of the war. After May of 2003, however, events turned against the US and psychological operations (PSYOP) and its PSYWAR effort did not do enough. Three lessons learned were that post-combat PSYWAR is an important part of PSYWAR operations; that the focal point of post-combat PSYWAR is psychological pacification of the broad masses and the psychological softening of any antagonistic forces; and that PSYWAR policy and tactics before, during, and after a war must be consistent both toward the domestic population and international opinion.

US forces in Iraq demonstrated that PSYWAR plays a key role in political, military, and diplomatic struggles. They made breakthroughs in PSYWAR since they held the political banner of antiterrorism, they diplomatically used mediation to isolate Iraq, and they threatened Iraq militarily. The comprehensive effect of these measures was that the Iraqi military and people felt an increased psychological burden, which hastened their collapse. The US controlled all dimensions of the war which meant they controlled the attitudes and beliefs of the domestic population and enemy morale.

Ai adds that PSYWAR must have depth and be present on the strategic, campaign, and tactical levels. Strategic commanders stress guidance, campaign commanders stress scheming, and tactical commanders stress planning according to Ai. This is a cause and effect affair that must be mutually supportive, coordinated, and complementary.

Ai postulated that Sun Tzu's ideas on PSYWAR must permeate all dimensions of war. To balk the enemy's plans, Ai recommended the use of PSYWAR deterrence, PSYWAR deception, and PSYWAR propaganda. "Shock and awe" was seen as a refurbished version of Sun Tzu's PSYWAR theory of shock and awe [note: this author is unaware to what Sun Tzu lesson Ai is referring.]. Another lesson learned was that everything should be done not only to balk enemy plans but also to prevent the junction of enemy forces. To accomplish these two issues it is

necessary to make contact, dialogue, exchange ideas, and communicate to change the other side's attitudes and resolutions.

The US based their policy solely on military force and this backfired on them. In Afghanistan, it was clear that when the US entered they had little cultural awareness and relied too much on military force. Psychological warfare personnel did not compose convincing messages and in some cases promoted terrorism unwittingly (for example, one leaflet warned and threatened the Taliban with death. However, since death is a way to see Allah, the Taliban were not intimidated. The words crusader and justice were also used in speeches and broadcasts and this was an affront to the Muslim world, since only Allah could provide infinite justice.).

Another lesson learned from US forces in Iraq is that it is easy to invade but difficult to occupy, and it is easy to attack cities but difficult to attack mentalities. Fighting and winning is not the same as fighting and convincing; and the results of conquering by military force are temporary while the results of conquering by psychology are permanent. PSYWAR as a national strategy should be understood as PSYWAR policy, tactics, measures, and actions for national politics, military affairs, economics, diplomacy, and culture.

Three problems warrant attention for China. First, a strategic think tank for PSYWAR is becoming increasingly important. Second, it is necessary to see the overall strategic situation when making plans. How PSYWAR is integrated into the overall plan is important. Finally, one must make simultaneous and composite use of many kinds of measures. There are also five faults that can endanger a military General: recklessness, cowardice, a hasty temper, a lack of honor, and over-soliciting his men, leading to worry and trouble.

Ai noted that war is not just about the use of force but also about the use of wit, most importantly the use of form, deception, and falsehood. Form is the basic operational intent of commanders to carry out PSYWAR activities. Deception involves varying the actual situations of terrain and military formations. Deception usually glimmers with Sun Tzu's wisdom of form. Ai believes the US military used deception and form very well as it moved from the south to the north in Iraq.

Today, Sun Tzu's ideas on deceptive PSYWAR contain three points for consideration. First, a flat form must be changed to a three-dimensional model containing hyperspace and range. Second, there are now comprehensive forms and not just a single form. Great use must be made of high-tech acoustics, optics, electronics, smoke, shadows, and images. Finally there is now a 24-hour form of military activities that is different from the past division of peace and war. This form permeates both peace and war.

In the end a righteous war is the backbone for PSYWAR. It provides the initiative for PSYWAR, and it causes the people to be in accord with the ruler and encourages them to follow him regardless of the danger. Ai believes US PSYWAR lost its foundation after the initial fighting because it had lost its righteous cause. PSYWAR could not be brought into play. Whereas Western strategic culture uses power to gain victory, Eastern culture uses strategy. This allows for the use of PSYWAR where inequity and imbalance are present. PSYWAR in such instances can permeate, neutralize, and influence.

Sun Tzu's Thoughts on War and Reflections on Informationized War[\[722\]](#)

Jiang Lei, from the PLA's Navy Command Academy, offered an interesting view on information war in general and the meaning of Sun Tzu's theory in the information age in particular. He noted that informationized warfare has introduced new patterns and new forms of warfare where crisis and peace are more intertwined than before. Decapitation operations are one such form. They take advantage of Sun Tzu's notion to "begin by seizing something that your opponent holds dear." Now warfare has become a confrontation between setups, between systems, and between networks. Systems can now determine the course of a war and enable victory or defeat. Informationized war is a trial of strength of the knowledge and action capabilities of both sides. The side with knowledge can see through the fog of war better than the other side and firmly control war's initiative and information supremacy, the latter being the key to victory in war.

But Jiang states that the basic character of war hasn't changed (wars will still be just or unjust, war will breed unpredictable consequences, etc.). He noted that

The new forms of informationized warfare... have not created a new modality for realizing the political objectives of warfare or new methods for preventing the disaster of war... the fundamental and crucial reason lies in the political objectives and nature of war, and it does not lie in changes or an escalation in the methods or forms of warfare, regardless of actual strength or technology...

Jiang concedes that wars can be shortened, casualties reduced, and precision destruction increased.

Major powers may think it is easier and more advantageous to launch wars due to these latter criteria. War seems more "doable." Jiang warns that war still has unexpected consequences that should make any major power hold back on the use of an informationized force. For example, an information force will drive smaller opponents to adopt extreme, irrational measures, or terrorist type methods of response and retaliation. Jiang quoted Sun Tzu, stating "he will win who knows when to fight and when not to fight. He will win who knows how to handle both superior and inferior forces."

To keep unexpected consequences from happening, Jiang recommends that major powers pay extra attention to Sun Tzu's guidance. Major powers should be more careful and not think that warfare has become easier. They should not put troops in the field to satisfy their own ego. They should also be careful not to go after primary decision makers since a series of unknown consequences could follow and responsibility for the main consequences of war will rest on the major power's shoulders. He quotes Sun Tzu, stating that "one may know how to conquer without being able to do it. He will win who, prepared himself, waits to take the enemy unprepared."

Sun Tzu's Strategic Thought and Its Inspiration for Informationized Warfare[\[723\]](#)

Author Chai Yuqiu of the Nanjing Army Command Academy divided his paper into two

parts. The first part covered the historical significance of Sun Tzu, and the second part discussed six ways that Sun Tzu's writings were relevant in the information age. Initially, Chai noted how Sun Tzu utilized what he termed "naïve materialistic and dialectic thought." This was embodied in Sun Tzu's discussions of the offense and defense, the direct and the indirect, advantages and disadvantages, night and day, work and rest, and so on. He called Sun Tzu a grand strategist without parallel in history.

Chai noted that Sun Tzu fused the thought of Confucianism, Daoism, Legalism, and Mohism and absorbed the laws of many professions. These included industry, agriculture, commerce, medicine, and military laws.

Regarding Sun Tzu's applicability today, Chai noted that the "quintessence of knowledge is wisdom, and the quintessence of wisdom is strategy." While knowledge can become antiquated with the passage of time, strategy cannot. That is why history is so relevant even today. It embodies the use and methods of strategy from the past.

Chai's six ways to use Sun Tzu's thinking include the following:

- "Breaking the enemy's resistance without fighting" is the ultimate goal of informationized warfare.
- "Knowing victory" is a prerequisite for being the first to win and gain a complete victory in informationized warfare.
- "Direct and indirect" warfare is revealed and developed even more in informationized warfare.
- "Quick decision" is the inevitable choice for informationized warfare in the pursuit of benefits in war.
- "Modifications and changes" have an even greater real significance in informationized warfare.
- "Psychological attack" has an even greater inspirational role in informationized warfare.

"Breaking the enemy's resistance without fighting" is reflected primarily in the planning of the offensive. However, in the information age, an offensive can mean a fighting method that doesn't spill blood or that doesn't depend on the use of force. Sides engaged in conflict in the twenty-first century will attempt to protect their own forces and yet produce a victory that is complete. This can be accomplished with informationized warfare and is the result that is sought by both sides.

"Knowing victory" refers to knowing several important things about an enemy. One must fully understand information in order to deliver victory. This means knowing the evils of war, a profitable way of conducting war, the army's condition, the power of opposing armies, the place and time of battle, enemy plans, the devious and the direct methods of attacking, the designs of the enemy and your neighbors, and the advantages accompanying one's tactics, among other issues. The side that controls the power to gain, use, and control information will be prepared to analyze and decide how to use one's own forces.

“Direct and indirect” refers to using the correct type of tactics for the force at one’s disposal. One must learn how to bring into play one’s own strengths and how to spot enemy weaknesses. Information age technologies can make the weak very strong.

“Quick decision” is a Sun Tzu thought that emphasizes the need to avoid prolonged warfare and exhausting one’s strength. Even in the information age it is important to stop expending large sums of money over extended periods of time. The expense of modern weapons can cause financial losses to happen quickly. Therefore quick victories are needed, even in the information age.

“Modifications and changes” emphasize that one side should not be constrained by conventional methods of fighting. One must adapt to crises and take appropriate actions. Even in the information age it is necessary for commanders to master changes in situations on the enemy’s side and one’s own side, the situation on the ground, and situations elsewhere in order to make timely decisions and to seize the initiative and victory.

“Psychological attack” depends on studying moods and awaiting the appearance of chaos or disorder. The same views hold in the information age. Only the methods have changed.

Today, no matter what the profession (politics, diplomacy, market operations, economic, or physical competition), strategy is still relevant. It is the only key to determining success or failure. Economic globalization, the use of high-technology by militaries, and the development of multivariable competition among businesses all indicate that strategies using information and information technologies will be part of our present and immediate future.

Abstracts of a Few Papers Not Issued[724]

Yu Jiang and Xiong Yuxiang of the PLA’s Academy of Military Science stated that PSYWAR has never been abandoned, even in the age of high-technology. Therefore Sun Tzu’s well-known thesis that “The ‘Qi’ of the three Armies can be snatched away and the commanding general’s mind can be seized” is still applicable. In fact, PSYWAR has become “wars outside wars and wars on top of wars.” It is a strategic means to realize national interests. Today PYSWAR has greater attack potential and its means are more diversified.

Author Zhang Zhiping of the Chinese Air Force’s Command College wrote that “subduing” is the core and essential aspect of Sun Tzu’s Art of War. Today aerospace power armed with information is the leading actor on the modern warfare stage, and it is the main method to subdue an enemy. An aerospace “net of awareness” can dispel the fog and friction of war. Complete victory can be obtained from afar. Aerospace power can be applied flexibly. It is the optimal way to deal with local wars and conflicts.

Finally, Wang Huqiang of the PLA’s Shenyang Military Area Command noted that Sun Tzu pays great attention to the effect of strategy in war. Deception becomes the golden rule guiding strategy. It is focused on avoiding strength, striking weaknesses, and using extraordinary force to win. Even in the age of information weapons, it is possible to find weaknesses in an enemy force. These weak points must be exploited and countermeasures worked out to strike them.

APPENDIX FOUR: DISCUSSION OF THE FORMS OF INFORMATION WARFARE

The following is a direct translation of a section of Chapter Three, “Total Emergence of Troop Combat Strength Systems,” pp. 109-121, of the book Discussion of Forms of Information Warfare by Dong Zifeng. The book was published by the PLA Publishing House in Beijing in 2004. It describes a way of looking at the combat strength of a unit under conditions of “informationization.” This portion of Dong’s book was translated by a private company.

IV. A Dynamics Equation for Military Combat Strength “Quantization”

The question of quantitative assessment of military combat strength has always been a difficult point in military science research. From Carl von Clausewitz’s quantity formula to Lanchester’s equation and T. N. DuBois’ new square law, military theorists over the world have done vast amounts of work to establish a series of mathematical models with definite results. For most of these models, however, a “metal-ized,” “gunpowder-ized,” and mechanized military is the object of the research, and they are set up on the foundation of combat strength as a continuous function. It cannot explain the “quantization” phenomenon of combat strength, nor can it resolve the issue of the emergence of combat strength brought on by the information structure. It is no longer suited to the reality of an “informationized” military. Based on the basic thinking of the quantitative characterization above, we have set up a combat strength “quantized” dynamic equation followed by a general discussion of the equation.

1. Combat Strength Quantum Mathematical Model

The combat strength quantum is a basic component unit of the informationized military combat strength system. It is a systematic mechanism established with the network as its core, information as the key element, and the information chain as the foundation, and it integrates the system of the traditional combat strength key elements and transforms it from platform-centered combat to network-centered combat.

The combat strength quantum should have the following basic characteristics: (1) independent fighting functionality; (2) capability to communicate within and without; (3) ability to receive outside information in an unsealed network; (4) changeable structure that, when the information chain is broken, can switch from an information network structure to a mechanical linear system; (5) under normal linked circumstances, the outside function and effectiveness of a combat strength quantum of any component form gradually tends to converge and become equivalent, but the value obtained is not continuous; (6) possession of one information advantage, a transparent battlefield, and direct-aim firing as a possible equivalent.

First, we examined the classic Lanchester equation for modern combat[725]:

$$\begin{cases} \frac{dx(t)}{dt} = -\alpha y(t) \\ \frac{dy(t)}{dt} = -\beta x(t) \end{cases} \quad (3.1)$$

In the formula, $x(t)$ and $y(t)$ each represent the time t for the survival number of the two sides' combat members after combat has begun; α and β are the coefficients of the proportion of casualties, respectively representing the average rate of combat member demise of the opposite side for Y and X. This differential equation shows that the proportion of casualties for one side of combat members is directly proportional to the number of combat members of the opposite side that are firing at that time. This conclusion implies the following assumptions:

- Each side has combat members using only one of the same type of weapon, that is, they have the same combat function and combat effectiveness.
- There are a sufficient number of combat members to act as continuous variable handling.
- The combat members of both sides are exposed, information is completely symmetrical, and they are in effective firing range of the opposing side's weapons.
- The combat members of each side all know the position of the other friendly members, and there will be no accidental casualties.
- Straight-aim firepower of members of the opposing side is evenly distributed, and they can immediately carry out a precise appraisal of the combat results and determine which of the opposite side's targets have already been destroyed.

Based on the military combat strength quantization assumptions and the basic characteristics of the combat strength quantum, other than the potential for incorrect symmetry of information on the informationized battlefield, the circumstance of network-centered combat[726] is the assumption criterion of the Lanchester equation. This has made it possible for us to use the Lanchester combat theory to establish a combat strength quantum mathematical model. In view of the fact that the square law combat model is appropriate for describing the military strength changes in modern combat straight aim warfare, its proportion of casualties coefficient primarily reflects the effect of the C⁴ISR system on straight-aim firing. We have used the Lanchester square law combat model after adjusting it:[727]

$$\begin{cases} \frac{dr}{dt} = -n_b \frac{R_{kb}^2}{K_{3b}R_{lb}^2} \frac{K_{1b}}{K_{2b}} b \\ \frac{db}{dt} = -n_r \frac{R_{kr}^2}{K_{3r}R_{lr}^2} \frac{K_{1r}}{K_{2r}} r \end{cases} \quad (3.2)$$

In the formula, r and b are the respective times t of the military strength of the two sides, red and blue; n_r and n_b are the respective tactical firing rates of the two sides, red and blue; R_{kr} and R_{kb} are the respective weapon casualty radii for the two sides, red and blue, and R_{lr} and R_{lb} are the respective indeterminate radii for the opponent target positions of both sides, red and blue; K_{1r} and K_{1b} are the target information resolution rate coefficients for the two sides, red and blue, where $K_1 \geq 1$; K_{2r} and K_{2b} are the combat result assessment rate coefficients for the two sides, red and blue, where $0 < K_2 \leq 1$; and K_{3r} and K_{3b} are the target discovery delay coefficients for the two sides, red and blue, where $0 < K_3 \leq 1$. Under conditions of a precision attack, $R_{kr} = R_{lr}$, $R_{kb} = R_{lb}$, and (3.2) can be simplified as:

$$\begin{cases} \frac{dr}{dt} = -n_b \frac{K_{1b}}{K_{3b}K_{2b}} b \\ \frac{db}{dt} = -n_r \frac{K_{1r}}{K_{3r}K_{2r}} r \end{cases} \quad (3.3)$$

When t is set equal to zero for both sides, the initial military strength of the two sides, red and blue, is r_0 and b_0 . For the sake of simplicity, assuming that the C⁴ISR system only affects the casualty coefficient of the red side against the blue side, then the military strength multiplication coefficient after using the new C⁴ISR system for the red side is:

$$G_R = \frac{r_0}{r_{0c}} \bigg|_{b(0) = b_0} = \sqrt{\frac{a_c}{a_0}} \quad (3.4)$$

Achieving given combat results

In the formula, a_c is the casualty coefficient after using the new C⁴ISR system, a_0 is the casualty coefficient before using the new C⁴ISR system. Using formulas (3.2) and (3.4), G_R can be obtained. Similarly, the military strength multiplication coefficient G_B for the red side against the blue side can be obtained.

The combat strength quantum is calculated based on the following formula:

$$P_n = G_R P_m \quad (3.5)$$

In the formula, G_R is the military strength multiplication coefficient, P_m is the combat effectiveness before informationization of the combat unit which can be obtained from the combat effectiveness index of the key elements that make up the combat unit. In addition, the average value

of the entire troop combat effectiveness indices can be obtained, but this does not take into consideration their specific calculation problems.

2. Mathematical Model for Information Structural Strength

(1) *Required Assumptions*

First, in peacetime, there is sufficient time to set up and informationize a troop combat strength system, far longer than in wartime. In wartime, the wartime period is sufficiently short, far less than the recovery time for an informationized troop combat strength system, and the ability to transform war potential into actual military strength is limited. For these reasons, the growth process of troop combat strength can be seen as a continuous growth process, and chaotic phenomena such as “branching off,” which is a continuous process of dispersal, exist with the disintegration of troop combat strength.

Second, under a network structure, the combat strength of a platform medium system is relatively constant. Creation of information structure strength is based on the chain movement of the information platform, digital chain, and information factors. With regard to single soldiers and weaponry itself, the informationizing process is an information factor embedding process; therefore, it is natural that weaponry and soldiers that have been remolded through informationization will have higher combat effectiveness and strength than originally. For example, some sensors that have higher attack precision are installed in guided missiles. What we are even more concerned about, however, is the problem of the leap in combat strength of these combat units acting under networks composed of particles, or the problem of information structural strength. To make analysis of this problem easier, then, we have converted the combat effectiveness before “particle-ization” into a corresponding combat effectiveness *CEV*, and in this way the combat strength of the combat unit under the network structure is constant and becomes a constant, P_m .

(2) *Metcalfe’s Leap*

Information structural strength is an independent increment, and its size follows the “Metcalfe Law.” Information structural strength is formed on the basis of the information platform network structure after the warfare unit has been fully particle-ized. Under these circumstances, we treated each combat strength quantum as a nodal point on the network and observed and studied the number of nodal points and changes in the system structural strength caused by differences in the relationships between them. We did not focus on the structural and operating processes inside the nodal points. However, this partial increase in value exceeds the P_n value independent increment, and we called it “Metcalfe’s Leap.” It is expressed in the following formula:

$$\Delta P_s = kP_n T^2 \tag{3.6}$$

In the formula, P_n is the combat strength exponent of the combat strength quantum; T is the combat strength quantum number within the effective battlefield space, that is, the network nodal point

number, and the solid space derived from the battlefield space, the upper limit of which is the altitude that the satellite reaches, and the distance from the earth's surface is 120,000 meters; k is the network structure correction coefficient (between 0 ~ 1) determined by the structure between the nodal points, and its expression is the level of troop informationization for which different values are taken from each of the different network connection methods as Internet, Web, and Grid and are determined by the "Hall for Workshop of Metasynthetic Engineering" (HWMSE). Under ideal circumstances of normal exchange of Internet interoperability, the value of k is 1.

(3) *Information Structural Strength*

The Metcalfe Leap for the combat strength system of the entire military refers to the information structural strength, and its size is:

$$\Delta P_I = \sum_{j=1}^T \Delta P_{sj} = \sum_{j=1}^T k P_{nj} T^2 \quad (j = 1, 2, \dots, T) \quad (3.7)$$

3. Formula for Calculation of Troop Combat Strength under Different Media Systems

When there are phase transformations in the troop combat strength system, the changeover of the system structure is carried out according to the following model: (1) In keeping with the component principles of an open, complex, huge system—troop combat strength is determined by the quality and quantity of the elements of combat strength as well as by the system structure, i.e., the interrelationship between the combat strength quantities. (2) The growth process for combat strength of informationized troops can be explained as a time continuous function $P = f(M, E, I)$, but the decay happens suddenly, and combat strength immediately disintegrates. "Quirks" exist in the system, and this turning point is the critical value in the loss of combat strength quanta. (3) The growth process of the combat strength of informationized troops is different than the path of quantization disintegration; when there are too many network nodal points, i.e., when combat strength quanta are too many, the system has redundancy and compensation; when disintegration occurs, it does not happen in reverse of the growth process. The regional area encompassed by combat strength growth and disintegration reflect the ability of the troop combat strength system to resist attack; the smaller the area, the weaker the system, and vice versa. (4) This type of troop combat strength disintegration is changeover of the system structure, i.e., a phase transformation. The human warfare medium system has undergone the three processes of fraternal media (substance), platform media (capability), and network media (information) and, therefore, in a war or battle, there exists the potential for three types of system structures in the troop combat strength system. When the information factor is fractional, it switches to the capability system; when the capability factor is fractional, it switches to the substance system; when the substance factor is fractional, the troops have completely lost their fighting capacity.

The formula for calculating troop combat strength under circumstances of the different media systems is as follows:

- (1) The substance system is the same as the cold weapon troop combat strength system,

and the combat strength unit for the system is 1 person + 1 weapon. The combat strength for the entire force is:[\[728\]](#)

$$P_0 = N \cdot V \cdot Q \quad (3.8)$$

In the formula, N is the number of troops for one of the battle opponents, V is the factor variable for conditions of one of the battle opponents, and Q is the quantified value of the troop quality of one of the battle opponents.

(2) The capability system is the same as the thermonuclear weapon troop combat strength system, and its combat strength unit is 1 person (certain person) + 1 platform + voice communication system. The combat strength for the entire force:[\[729\]](#)

$$P_E = S \cdot V_f \cdot CEV \quad (3.9)$$

In the formula, S represents the troop military strength; V_f represents the troop military strength variable, which is determined by the environment variable, war variable, and action variable; CEV represents the corresponding battle effectiveness index. Of these, the military strength S is the total value of the actual operational lethality index of each type of weapon that an army has after taking into account the effect of special battlefield conditions on the usage results of this type of weapon:

$$S = \sum_{i=1}^n W_i V_i \quad (i = 1, 2, \dots, n) \quad (3.10)$$

In the formula, W_i is the total value of the actual operational lethality index (OLI) of a specific weapon, and V_i is the factor affecting the effectiveness of the specific weapon. The actual operational lethality index is:[\[730\]](#)

$$OLI = \frac{TLI}{DI} \tau \quad (3.11)$$

In the formula, TLI is the theoretical lethality index, DI is the dispersal factor, and τ is the performance factor for each weapon. TLI is determined from the following formula:

$$TLI = RF \cdot R \cdot A \cdot C \cdot R_n \quad (3.12)$$

In the formula, RF is the rate of fire, R is the reliability, A is the accuracy, C is the target hit number of each firing, and R_n is the firing range. It is worth noting that, under conditions of an informationized battle, DI should be solid space.

The combat effectiveness value, CEV , is derived from the following formula[\[731\]](#):

$$CEV_r = (R_r/R_b)/(P_r/P_b) \quad (3.13)$$

In the formula, CEV_r is relative combat effectiveness value of the red side, R_r/R_b is the actual battle result of the red side against the blue side, which is the ratio of the two sides' actual combat strength; P_r/P_b is the theoretical battle results of the red side against the blue side, which is the ratio of the two sides' combat potential. Of these, the battle results R_r (or R_b) are derived from the following formula:

$$R_r = MF + E_{sp} + E_{cas} \quad (3.14)$$

In the formula, MF is the mission factor, which reflects the capability of an army to achieve its accepted mission or self-understood mission as determined by military specialists; E_{sp} is space performance, which measures the capability value of an army to capture or hold a position; E_{cas} is the casualty results, and it is the combat strength of an army measure on the basis of the casualty rate.

The combat strength quantum basic battle effectiveness index is:

$$P_m = \frac{P_E}{T} \quad (3.15)$$

In the formula, T is the combat strength quantum number in the battlefield space.

(3) The information system is the structural characteristic of an informationized army. A mature informationized army or mature digitized battlefield has a normally linked network, the chain of information movement is unimpeded, and, after the battle unit is particle-ized, a combat strength quantum is formed with diffuse distribution on the battlefield, thereby causing a leap in the combat strength of the army to follow Metcalfe's law." For these reasons, the combat strength of an informationized army should be composed of two parts – one part is the sum of independent combat strength quanta, and the other part is the information structural strength produced by the networked combat strength quanta. From formulas (3.5), (3.7), and (3.15), we get:

$$\begin{aligned} P_I &= P_E + \Delta P_I = P_E + \sum_{j=1}^T k P_{nj} T^2 = P_E + k G_R P_E T^2 \\ &= P_E (1 + k G_R T^2) \quad (j = 1, 2, \dots, T) \end{aligned} \quad (3.16)$$

4. A Variable Structure Mathematical Model for the Combat Strength System of an Informationized Army

From the previous analysis, we know that the combat strength system of an informationized army actually implies three types of structures: (1) The hand-foot intermediary

system with substance as the guiding factor; (2) the platform intermediary system with capability as the guiding factor; and (3) the network intermediary system with information as the guiding factor. They each correspond to physical-centered war, platform-centered war, and network-centered war of the human war intermediary system in revolutionary history. The following system of equations is obtained when formulas (3.8), (3.9), and (3.16) are linked:

$$\begin{cases} P_0 = N \cdot V \cdot Q & T = 0, \quad k = 0 \\ P_E = S \cdot V_f \cdot CEV & T = 1, \quad k = 0 \\ P_I = P_E(1 + kG_R T^2) & T \geq 2, \quad 0 < k \leq 1 \end{cases} \quad (3.17)$$

Formula (3.17) is the variable structure mathematical model for the informationized troop combat strength system.

The required discussion is carried out below in order to deepen understanding of its military significance.

(1) Formula (3.17) shows that, during the process of informationizing an army, the structure of the military system is variable. When the combat strength quantum number T is greater than 2, when the networking coefficient $k \neq 0$, the military system is at the network-centered war structure, Metcalfe's Leap exists, and the army combat strength system engenders information structural strength. When the combat strength quantum number $T = 1$, and the networking coefficient $k = 0$, $P_I = P_E$, and the military system is transformed into a platform-centered war structure. When the combat strength quantum number $T = 0$, and the networking coefficient $k = 0$, this means that the army system has lost its capacity and support of the information factor, and the military system has transformed into a physical-centered war structure and entered face-to-face combat with hands-and-feet as the intermediary.

(2) If the combat strength quantum number T is large enough, P_E can be overlooked and, therefore, we can deduce the formula for the army combat strength system battle effectiveness index under conditions of a mature network system:

$$P_I = kG_R P_E T^2 \quad (3.18)$$

The formula above shows that, under ideal conditions of complete informationization, networking, and "intellectualization," the army combat strength comes primarily from the information structural strength, and it becomes a direct proportion with the square of the number of combat strength quanta. This is precisely the description of Metcalfe's Law.

(3) In the simultaneous set of equations, the formula for calculating P_I is actually the dynamic formula after the growth process of an informationized army combat strength is completed. During the course of a war, if the war time t is short enough, and the combat strength quantum number T is large enough, then P_I can be seen as a continuous function that follows the changes in T . The following is derived from formula (3.18):

$$\frac{dP_I}{dT} = -2kG_R P_E T \quad (3.19)$$

The formula above shows that disintegration of the combat strength of an informationized army declines linearly with the combat strength quantum number. If it is assumed that the two sides are both carrying out resistance using network-centered combat, then the following equation is obtained:

$$\begin{cases} \frac{dP_{I_r}}{dT} = -2k_b G_b P_{Eb} T_b \\ \frac{dP_{I_b}}{dT} = -2k_r G_r P_{Er} T_r \end{cases} \quad (3.20)$$

resulting in:

$$\begin{cases} \xi = 2k_b G_b P_{Eb} \\ \theta = 2k_r G_r P_{Er} \end{cases} \quad (3.21)$$

to obtain:

$$\begin{cases} \frac{dP_{I_r}}{dT} = -\xi T_b \\ \frac{dP_{I_b}}{dT} = -\theta T_r \end{cases} \quad (3.22)$$

With minor conversion, [\[732\]](#) the following can be derived:

$$\xi T_b^2 = \theta T_r^2 \quad (3.23)$$

In the formula, θ and ξ are the network casualty coefficients for the red and blue sides, respectively, against their opponent. T_r and T_b are the combat strength quantum numbers for the red and blue sides, respectively. Formulas (3.22) and (3.23) are derived from Metcalfe's Law, and are isomorphic with Lanchester's square law. We have called it the "Metcalfe-Lanchester Equation." The military significance of the Metcalfe-Lanchester Equation is obvious – it shows that, under network-centered war conditions, the combat strength disintegration of both fighting sides is determined by the product of the network casualty coefficient and the combat strength quantum number. This reflects the essential characteristics of an informationized war in the network-centered war phase attacking the structure and the nodal points. At the same time, compared with the α and β values, the θ and ξ values are much larger, which shows that, under conditions of an informationized war, troop combat strength will rapidly change in keeping with

the changes in the combat strength quantum number. This provides a theoretical basis for the phenomenon of “crumbling” combat strength.

(4) Because of the redundancy and complementation functions of a combat strength quantum network, the impact of the combat strength quantum number T on P_I is relatively small before arrival at the critical point, and it cannot be reduced according to the P_I growth locus, there exists a difference, ΔT , between the variable critical value T_P and the T_G value that corresponds to P_I in the growth process, as illustrated in Figure 3.1.

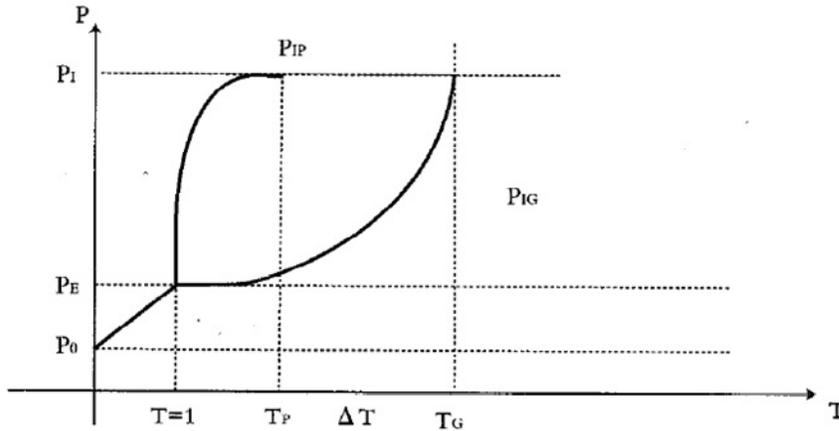


Figure 3.1 – Envelope
Curve Diagram of the Combat Strength of an
Informationized Army

In the diagram, the military significance of the area of the envelope curve formed by the rise and fall of P_I reflects the resistance fighting capability of an informationized army. As the area increases, the resistance fighting capability becomes stronger, and as the area decreases, the system surplus diminishes, and the resistance fighting capability becomes weaker. This means that, under network-centered war conditions, there exists a “virtual combat strength quantum” in the military system. In order to measure this capability of an informationized military system, we have introduced the combat strength quantum surplus coefficient ρ :

$$\rho = \frac{T_G}{T_P} \quad (3.24)$$

Because $\Delta T = T_G - T_P$, the system resistance fighting coefficient is:

$$\zeta = \frac{\Delta T}{T_G} = \frac{T_G - T_P}{T_G} = 1 - \frac{T_P}{T_G} = 1 - \frac{1}{\rho} \quad (3.25)$$

The formula above shows the relationship between the combat strength quantum surplus coefficient and the system resistance fighting coefficient such that when $\Delta T = 0$, $T_G = T_P$, and in

this case $\rho = 1$ and $\zeta = 0$, which shows that the system's resistance fighting capability is very poor, and the military system is very weak. With regard to one specific war or battle, establishment of many large-scale network-centered battles will obtain a suitable T value, which has decisive significance when using the smallest cost to get the greatest combat success. This advances the potential prerequisite conditions for the "intimidation theory."

(5) The system theory mechanism for the combat strength crumble phenomenon. In 1943, B. O. Koopman used the variable substitution method to get a square law format solution for the Lanchester equation (see formula [3.1]), and the results were published in 1963. Actually, we can directly derive its accurate solution directly from the Lanchester square law differential equation, and the result is a hyperbolic function set of equations.

We know that a hyperbolic function solution is characterized by accelerated process effect as it nears the conclusion. In the past, we generally used this to explain the reasons for the accelerated process during the period following a battle. "The time it took to annihilate the losing side during the second half of the battle unit is shorter than the annihilation time during the first half. This is because the winning side can concentrate the entire firepower of its battle unit on the remaining portion of the losing side and, therefore, speed up the annihilation." [733] Obviously, under conditions of a network-centered war, this is not complete because, from what we can see from the Metcalfe-Lanchester Equation, the information structural strength first needs to be considered in addition to the effect of the concentrated firepower. As long as the combat strength quantum number T for the entire war space is not less than the critical value, the army combat strength system will not experience a "collapse." Actually, this reasoning is obvious because, in a mature network-centered war, the distribution-type war will become the primary method, and it does not matter where the combat strength quantum is as long as the combat strength quantum network still exists. Just as the United States Army says, "By using advanced technology of the information age, the military can apply new military concepts of the information age in its work and realize distribution-type war by simply transmitting information rather than moving personnel, using information in place of goods and materials." [734]

(6) After the chain-type movement of information in an informationized army is cut off, and the system structure changes from a "network-type" to a "platform-type," how is it any different from the combat strength of an army that always was a platform-type mechanized army? In other words, can an informationized army that has lost its information platform fight as effectively as before it became informationized? This is the current question that must be answered and resolved by the changing structural system. Just as a newly established economic system will engender a corresponding systemic culture and form "method dependencies," [735] the establishment and development of an informationized military system will similarly engender certain dependencies on information platforms such as C^4 ISR and its command control models. Once an information platform encounters a destructive attack, whether tactical, technical, or psychological, people have the potential for not knowing which way to turn. As a result, the speed of the military system goes from a state of order to a state of disorder, and it loses its original combat capability. These circumstances exist for combat strength quanta and for the entire army and pose an important question for war and training: How do you make an army adapt to these changeovers to the system structure during peacetime military training, and how do you answer to these changeovers in wartime war battle plans?

In research of the forms of informationized warfare, we found that the phenomenon of troop combat strength quantization needs to be explained using complex system theory and mathematical models. This only gives one type of formal dynamic formula, and there may be a different way of expressing it if a different mathematical tool is selected. We know that it is very difficult for any mathematical method to describe precisely an action rule for a troop combat strength system or accurately predict the outcome of a battle. Perhaps we will never find an army or a battle for which the actual circumstances completely coincide with the mathematical model border circumstances. However, a mathematical model can bring to light the basic characteristics of an army combat strength system, and at a minimum show the significance of changes to the components and structure of the army combat strength system in view of a system's emergence. In addition, these changes can also happen during the course of a battle, and this will have successfully explained the appearance of such phenomena as a leap in combat strength in an informationized military, the presence of combat strength crumbling in an informationized military, and the "algebraic" law of diminishing weapons, the reasons for which can be the presence of low-grade weapons, different usage conditions for different weaponry, different usage phases, and different usage targets. On the whole, a general rule for quantitative recognition of the system's emergence allows us to deeply grasp the substance of the informationized military revolution and equitably build and use the army to our benefit.

DEDICATION

This book is dedicated to my children, Sally, Michael, and Matthew; and to my wife, Christine, who reviewed the manuscript and made it much better. I thank my children for their encouragement, support, and help along the way, and I thank my wife for her patience and willingness to ask probing questions that enabled me to get at the essence of Chinese IW.

ACKNOWLEDGEMENT

The author used only open-source translations for the construction 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 Chinese translators in order to write this book. The author is solely responsible for the selection and analysis of the material others translated.

In particular, the author would like to acknowledge the support of five individuals who assisted with this project. First, and foremost, is Navy Senior Chief Bart Zobel of the Navy Reserve Navy Information Operations Command who is responsible for much of the translation support. Chief Zobel translated the entire contents of both On the Chinese Revolution in Military Affairs and An Interpretation of Network Centric Warfare. He translated nearly half of the contents of Deciphering Information Security and selected sections of Direct Information War. Without his assistance, this work would not have been possible to assemble. Second, the author would like to thank Mr. Charles A. Martinson III of Fort Leavenworth who designed the cover artwork. Mr. Martinson's visualization of the contents of this book is unique. His creativity is truly his trademark. The author would like to thank SPC Hommy Rosado and Mr. Randy Love of the Foreign Military Studies Office. SPC Rosado is responsible for the graphic work on tables found at the end of Chapters One and Two. Mr. Love monitored commercial translations of some material used in this work. Mr. Karl Prinslow, Acting Director of FMSO, ensured that funding for the translation of all Chinese material was available.

Finally, the author would like to express his thanks to the Air Force Information Center in San Antonio, Texas for providing the financial support behind the printing of this book. Without their support this work would never have reached the multitude of analysts studying this topic.

NOTES

- [1] Nathan Thornburgh, "The Invasion of the Chinese Cyberspies," Time, 29 August 2005, downloaded from <http://www.time.com> on 23 January 2007.
- [2] Vago Muradian, "China Tried to Blind US Sats with Laser," Defense News, 25 September 2006, p. 1.
- [3] Josh Rogin, "Network Attack Disables Naval War College," Federal Computer Week, 30 November 2006, downloaded from <http://www.fcw.com>.
- [4] Anthony Kuhn, National Public Radio, 19 January 2007, interview with Beijing representative.
- [5] "Chinese Hackers Attack Taiwan Military Computers," Taipei P'ing-kuo Jih-pao (Internet Version) 15 May 2006, as reported in Open Source Center report CPP20060516310002.
- [6] This author reviewed Peng and Yao's The Science of Military Strategy and credits the content, concepts, and ideas to the book's editors and authors of the individual chapters. The content of the book is reviewed based on translated material. Translation credit belongs to the PLA.
- [7] Peng Guangqian and Yao Youzhi, editors, The Science of Military Strategy, Military Science Publishing House, Academy of Military Science of the Chinese People's Liberation Army, English version, 2005, p. 32.
- [8] Stratagem generally refers to scheming and military strategy (or tactics—taolue); the war planning (or scheme, plot—mohua) employed by the two opposing combatants to be used at different levels of military strategy, military campaign, and military tactics in order to obtain victory. Military stratagem is a product of the development of war, the concrete manifestation of human subjective actions upon material forces. It reflects the general principles of military struggles, possessing a corresponding stable nature and vigorous liveliness. See the Chinese People's Liberation Army Officer's Handbook, Qingdao Publishing House, June 1991, p. 197.
- [9] Wang Xingsheng, "Chinese Intellectuals Paying Close Attention to Military Issues: Tradition and Its Impact on Military Culture," China Military Science, 2002, No. 6, pp. 23-27.
- [10] Ibid.
- [11] The Chinese note on page 492 of The Science of Military Strategy that the term informationization is the same as cyberization. The author will use informationization in this text but the reader may insert the more familiar term cyberization in its place.
- [12] Peng and Yao, p. 503.
- [13] Ibid.
- [14] Joint Publication 1-02, DOD Dictionary of Military and Associated Terms, 12 April 2001, downloaded from <http://www.dtic.mil/doctrine/jel/doddict/index.html>, for all terms as amended through 31 August 2005.
- [15] Ibid., as amended through September 2006.
- [16] Chinese Military Encyclopedia, Vol. 3, July 1997, p. 699.
- [17] Peng and Yao, p. 130.
- [18] Ibid., p. 9.
- [19] Ibid., p. 10.
- [20] J. Boone Bartholomees, "A Survey of the Theory of Strategy," editor, US Army War College Guide to National Security Policy and Strategy, Second Edition, 16 June 2006, p. 81, as downloaded from the Internet on 5 July 2006 at www.au.af.mil/au/awc/awcgate/ssi/policy_strategy.pdf.

- [21] Ibid., p.110.
- [22] Peng and Yao, pp. 53-55.
- [23] Ibid., pp. 62-72.
- [24] Ibid., p. 9.
- [25] Ibid., pp. 15-17.
- [26] Ibid., p. 57. The three stages of protracted war were listed as the enemy's strategic offensive and friendly strategic defense, the enemy's strategic consolidation and friendly preparation for the counter-offensive, and friendly counter-offensive and the enemy's strategic retreat.
- [27] Bartholomees, pp. 387-389.
- [28] Ibid., pp. 389-390.
- [29] Ibid., p. 391.
- [30] Ibid., p. 390.
- [31] Peng and Yao, p. 2.
- [32] Ibid., p. 27.
- [33] Ibid., p. 5.
- [34] Ibid., p. 27.
- [35] Ibid., p. 94.
- [36] Ibid., p. 26.
- [37] Ibid., p. 28.
- [38] The words that served as the basis for this diagram can be found on pages 29-35 of the English version of The Science of Military Strategy.
- [39] Peng and Yao, p. 39.
- [40] Ibid., p. 30.
- [41] Ibid., pp. 39-44.
- [42] Ibid, pp. 55-62.
- [43] Ibid., pp. 62-72
- [44] Ibid., p. 31.
- [45] Ibid.
- [46] For a more detailed explanation of China's view of US culture, see Ren Xiangqun, "The Influence of Mainstream Cultural Traditions on US War Decisions," China Military Science, Issue 4, 2004, pp. 127-136. This is one of the best Chinese interpretations of US culture to appear in this journal.
- [47] Peng and Yao, pp. 72-77.
- [48] Ibid., p. 128.
- [49] Ibid., p. 126.
- [50] Ibid., p. 102.
- [51] Ibid., p. 104.
- [52] Ibid.
- [53] Ibid., pp. 104-107.
- [54] Ibid., p. 107.
- [55] Ibid., p. 130.
- [56] Ibid., p. 131. The Chinese military often use the term "strategic conductor." It can have singular or plural meaning.
- [57] Ibid., pp. 132-133.
- [58] Ibid., pp. 134-135.
- [59] Ibid., p. 135.

- [60] Ibid., pp. 136-137.
- [61] Ibid., pp. 138-143.
- [62] Ibid., p. 150.
- [63] Ibid., pp. 152-155.
- [64] Ibid., pp. 156-158.
- [65] Ibid., pp. 34-35.
- [66] Ibid., pp. 13-14.
- [67] Ibid., p. 59.
- [68] Ibid., pp. 59-60.
- [69] Ibid., pp. 15-18.
- [70] Ibid., pp. 336-337.
- [71] Ibid., p. 338.
- [72] Ibid., pp. 339-340.
- [73] Ibid., pp. 340-343.
- [74] Ibid., p. 344.
- [75] Ibid., p. 345.
- [76] Ibid.
- [77] Ibid.
- [78] Ibid., p. 336.
- [79] Ibid., p. 244.
- [80] Dong Zifeng, Discussion of the Forms of Information Warfare, PLA Publishing House, Beijing, 2004.
- [81] Peng and Yao, p. 306.
- [82] Ibid., p. 185.
- [83] Ibid., p. 172.
- [84] Ibid., p. 191.
- [85] Ibid., pp. 84-85.
- [86] Ibid., p. 184.
- [87] Ibid., p. 188.
- [88] Ibid., p. 180.
- [89] Ibid., p. 178.
- [90] Ibid., pp. 220-221.
- [91] Ibid., p. 18.
- [92] Ibid., p. 317.
- [93] Ibid., pp. 348, 349.
- [94] Ibid., p. 353.
- [95] Ibid., p. 323.
- [96] Ibid., p. 330.
- [97] This chapter appeared in English in the Number 3, 2005 issue of the Chinese Academy of Military Science's publication China Military Science.
- [98] Peng and Yao, p. 362.
- [99] Ibid., p. 372.
- [100] Ibid., p. 374.
- [101] Ibid., pp. 372-373.
- [102] Ibid., p. 374.
- [103] Ibid., p. 376.

- [104] Ibid., pp. 363-364.
- [105] Ibid., pp. 364-368.
- [106] Ibid., pp. 369-370.
- [107] Ibid., p. 471.
- [108] Ibid., pp. 397-398.
- [109] Ibid., p. 404.
- [110] Ibid., p. 447.
- [111] Ibid., pp. 448-449.
- [112] Ibid., p. 451.
- [113] Ibid., p. 406.
- [114] Ibid., pp. 435-439.
- [115] Ibid., pp. 453-454.
- [116] Ibid., p. 415.
- [117] Ibid., p. 455.
- [118] Ibid., p. 457.
- [119] Ibid., p. 459.
- [120] Ibid., p. 460.
- [121] Ibid., p. 415.
- [122] Ibid., p. 416.
- [123] Ibid., pp. 418-419.
- [124] Ibid., p. 425.
- [125] Ibid., p. 461.
- [126] Ibid., p. 420.
- [127] Ibid., p. 428.
- [128] Ibid., p. 432.
- [129] Ibid., p. 429.
- [130] Ibid., p. 470.
- [131] Ibid., p. 473.
- [132] Ibid., p. 164.
- [133] Ibid., pp. 170-171.
- [134] Ibid., p. 173.
- [135] Ibid., p. 177.
- [136] Ibid., p. 179.
- [137] Ibid., p. 189.
- [138] This chapter later appeared in English in the Number 6, 2005 issue of the Chinese Academy of Military Science's publication China Military Science.
- [139] Peng and Yao, p. 209.
- [140] Ibid., p. 197.
- [141] Ibid., pp. 199-200.
- [142] Ibid., pp. 202-204.
- [143] Ibid., pp. 205-206.
- [144] Ibid., pp. 207-208.
- [145] This chapter later appeared in English in the Number 5, 2004 issue of the Chinese Academy of Military Science's publication China Military Science.
- [146] Peng and Yao, p. 213.
- [147] Ibid., p. 215.

- [148] Ibid., p. 225.
- [149] Ibid., p. 226.
- [150] Ibid., pp. 227-228.
- [151] Ibid., p. 230.
- [152] Ibid.
- [153] Ibid., p. 232.
- [154] Ibid., p. 239.
- [155] Ibid., p. 244.
- [156] Ibid., p. 247.
- [157] Ibid., p. 293.
- [158] Ibid., p. 234.
- [159] Ibid., p. 237.
- [160] Ibid., pp. 248-249.
- [161] Ibid., p. 250.
- [162] Ibid., p. 251.
- [163] Ibid., p. 266.
- [164] Ibid., p. 266-267.
- [165] Ibid., p. 269.
- [166] Ibid., p. 274.
- [167] Ibid., p. 276.
- [168] Ibid., pp. 278-279.
- [169] Ibid., pp. 279-280.
- [170] Ibid., pp. 280-281.
- [171] Ibid., pp. 281-286.
- [172] Ibid., p. 287.
- [173] Ibid., pp. 288-293.
- [174] Ibid., p. 295.
- [175] Ibid., pp. 296-305.
- [176] Ibid., p. 305.
- [177] Ibid., pp. 307-308.
- [178] Ibid., p. 311.
- [179] Ibid., p. 313.
- [180] Ibid., pp. 313-314.
- [181] Ibid., pp. 315-316.
- [182] Ibid., pp. 318-320.
- [183] Ibid., p. 321.
- [184] Ibid., p. 323.
- [185] Ibid., p. 326.
- [186] Ibid., p. 327.
- [187] Ibid., pp. 330-331.
- [188] Ibid., p. 332.
- [189] Ibid., p. 347.
- [190] Ibid., p. 350.
- [191] Ibid., p. 351.
- [192] Ibid., p. 352.
- [193] Ibid., p. 356.

- [194] Ibid., pp. 377-380.
- [195] Ibid., p. 381.
- [196] Ibid., pp. 384-385.
- [197] Ibid., pp. 390-391.
- [198] Ibid., pp. 442-443.
- [199] Ibid., p. 445.
- [200] Ibid., p. 426.
- [201] Ibid., p. 427.
- [202] Ibid., p. 503.
- [203] Bartholomees, p. 107.
- [204] Bartholomees, pp. 83-84 and 93.
- [205] Harry Yarger, "Toward a Theory of Strategy: Art Lykke and the Army War College Strategy Model," in J. Boone Bartholomees, editor, US Army War College Guide to National Security Policy and Strategy, Second Edition, 16 June 2006, pp. 107-110, downloaded from the Internet on 5 July 2006.
- [206] David Jablonsky, "Why is Strategy Difficult?" in J. Boone Bartholomees, editor, US Army War College Guide to National Security Policy and Strategy, Second Edition, 16 June 2006, p. 115, downloaded from the Internet on 5 July 2006.
- [207] Jablonsky, p. 123.
- [208] This author reviewed Xu Xiaoyan's article in China Military Science and credits the content, concepts, and ideas to the article's author. The content of Xu's article is reviewed based on translated material. Translation credit belongs to the Open Source Center.
- [209] Bao Guojun and Guo Ruihong, "Great Achievements in All-PLA Military Scientific Research in the Period of the 10th Five-year Plan," Xinhua Domestic Service, 6 July 2006 as downloaded from the Open Source Center website on 18 July 2006.
- [210] Ibid.
- [211] Xu Xiaoyan, "Advancing the Science of Information Operations," China Military Science, Vol. 3, 2004, pp. 37-43. This article was taken from a FBIS translation, a translation that also does not list specific pages but only the "to-from" pages in the original Chinese document.
- [212] Ibid.
- [213] Ibid.
- [214] Ibid.
- [215] Ibid.
- [216] Ibid.
- [217] Ibid.
- [218] Ibid.
- [219] Ibid.
- [220] Ibid.
- [221] Ibid.
- [222] Ibid.
- [223] Ibid.
- [224] Ibid.
- [225] Ibid.
- [226] Ibid.
- [227] Ibid.
- [228] Ibid.

- [229] Ibid.
- [230] Ibid.
- [231] Ibid.
- [232] Ibid.
- [233] Ibid.
- [234] Ibid.
- [235] Ibid.
- [236] Ibid.
- [237] Ibid.
- [238] Ibid.
- [239] Ibid.
- [240] This author reviewed Shen Weiguang's On the Chinese Revolution in Military Affairs and credits the content, concepts, and ideas to the book's editor and authors of the individual chapters. The content of Shen's book is reviewed based on translated material. Translation credit belongs to Senior Chief Bart Zobel of the Navy Reserve Navy Information Operations Command.
- [241] Steven Metz and James Kievit, "Strategy and the Revolution in Military Affairs: from Theory to Policy," June 27 1995. As downloaded from the Internet at <http://www.dtic.mil/doctrine> on 29 August 2005.
- [242] Jeffrey Cooper, "War in the Information Age: The Changing Technology of the Battlefield," paper presented at a conference entitled "Rethinking Proliferation in the Post-Cold War Era," England, December 1995.
- [243] Richard O. Hundley, Past Revolutions, Future Transformations, RAND, 1999, footnote 12, p. 11.
- [244] Ibid., p. 9.
- [245] Wang Baocun, "China and the Revolution in Military Affairs," China Military Science, No. 5 2001, pp. 149 and 154.
- [246] Dai Qingmin, "Discourse on Armed Forces Informationization Building and Information Warfare Building," [this chapter appeared verbatim as an article in a 2002 China Military Science journal] On the Chinese Revolution in Military Affairs, ed. Shen Weiguang, New China Press, 2004, pp. 39-47.
- [247] Hai Lung and Chang Feng, "Chinese Military Studies Information Warfare," Kuang Chiao Ching, No 280, 16 January 1996, pp. 22-23 as translated in FBIS-CHI-96-035, 21 February 1996, pp. 33-34.
- [248] Zhang Feng, "Historical Mission of Soldiers Straddling the 21st Century," Jiefangjun Bao, 2 January 1996, p. 6 as translated in FBIS-CHI-96-061, 28 March 1996, p. 29.
- [249] Definition obtained by the author during a trip to China in 1997.
- [250] Cheng Yawen, "Keep Abreast of the Development Pattern of the New Military Revolution," Jiefangjun Bao, 7 July 1998, p. 6 as downloaded from the FBIS web page on 21 July 1998.
- [251] Senior Chief Bart Zobel of the Navy Reserve Navy Information Operations Command translated this book into English. The author is indebted to his linguistic talents and assistance that made this chapter possible.
- [252] Cheng.
- [253] Niu Li, Li Jiangzhou, and Xu Dehui, "Planning and Application of Strategies of Information Operations in High-Tech Local War," Zhongguo Junshi Kexue (China Military Science), No. 4, 2000, pp. 115-122 as translated and downloaded from the FBIS Website on 9 November 2000.

- [254] Li Bingyan, “Applying Military Strategy in the Age of the New Revolution in Military Affairs,” The Chinese Revolution in Military Affairs, ed. Shen Weiguang, New China Press, 2004, pp. 2-31.
- [255] Liu Yazhou, Qiao Liang, Wang Xiangsui—“Taking War to the Air and China’s Air Force,” The Chinese Revolution in Military Affairs, ed. Shen Weiguang, New China Press, pp. 48-62.
- [256] Li Bingyan.
- [257] Wu Chenguang, “China’s Advancing the New Revolution in Military Affairs,” On the Chinese Revolution in Military Affairs, ed. Shen Weiguang, New China Press, pp. 147-153.
- [258] Li Bingyan.
- [259] Ibid.
- [260] Ibid.
- [261] Ibid.
- [262] Li Bingyan.
- [263] Ibid.
- [264] Ibid.
- [265] Wang Baocun, “The Development of the New World Revolution in Military Affairs and its Strategic Influence,” On the Chinese Revolution in Military Affairs, ed. Shen Weiguang, New China Press, pp. 63-82.
- [266] Ibid.
- [267] Ibid.
- [268] Li Jijun, “The New Revolution in Military Affairs and Changes in Strategic Thinking,” On the Chinese Revolution in Military Affairs, ed. Shen Weiguang, New China Press, pp.32-38.
- [269] Ibid.
- [270] Wang Pufeng, “The Extent and Depth of the Worldwide Revolution in Military Affairs,” On the Chinese Revolution in Military Affairs, ed. Shen Weiguang, New China Press, pp. 83-90.
- [271] Ibid.
- [272] Tong Weibing, “The ‘New’ in the New Revolution in Military Affairs,” On the Chinese Revolution in Military Affairs, ed. Shen Weiguang, New China Press, pp. 91-95.
- [273] Li Bingyan.
- [274] Ibid.
- [275] Ibid. Situations that commanders’ talk about in military strategy refer to different locations in space and different distributions of forces. Creating a situation that strategy can exploit requires mastery of the following principles: high-position situations restrict low-position situations; external situations (exterior lines) restrict internal situations; network situations restrict satellite-point situations (force must be dispersed, extended, multi-point); one flank situations (focus flow of energy, grasping the heart of an operation) restrict multiple flank situations; “bearing” situations (those that are mutually codependent and interact—an example is ball bearings that play a role together) restrict “plate” situations (if you injure one, you injure all); and important-point situations restrict line situations and surface situations (“point” refers not to size but to the location in the overall situation—for example, the US’s 16 sea ports, as well as its high-technology campaign operations and precision attack are point operations).
- [276] Ibid.
- [277] Ibid.
- [278] Ibid.
- [279] Ibid.
- [280] Ibid.

- [281] Ibid.
- [282] Li Bingyan.
- [283] Ibid.
- [284] Ibid.
- [285] Dai.
- [286] Li Bingyan.
- [287] Li Bingyan.
- [288] Wang Pufeng.
- [289] Li Bingyan.
- [290] Ibid.
- [291] Dai.
- [292] Wang Pufeng.
- [293] Ma Yaxi, “A Few Thoughts on Advancing Military Informationization Building,” On the Chinese Revolution in Military Affairs, ed. Shen Weiguang, New China Press, pp. 96-104.
- [294] Li Bingyan.
- [295] Shen Weiguang, “Trends in the Development of World Warfare—Reducing destructive Force,” On the Chinese Revolution in Military Affairs, ed. Shen Weiguang, New China Press, pp. 131-146.
- [296] Li Bingyan.
- [297] Ibid.
- [298] Li Jijun.
- [299] Shen.
- [300] Li Bingyan.
- [301] Shen.
- [302] Ibid.
- [303] Wang Pufeng.
- [304] Dai.
- [305] Ma.
- [306] Wang Baocun.
- [307] Wu.
- [308] Qiao and Wang Xiangsui.
- [309] Liu, Qiao, Wang Xiangsui.
- [310] Ma.
- [311] Ibid.
- [312] Wang Baocun.
- [313] Dai.
- [314] Li Bingyan.
- [315] Ibid.
- [316] Ibid.
- [317] Tong.
- [318] Xie
- [319] Shen.
- [320] Qiao Liang and Wang Xiangsui, “Fully Calculating the Costs and Profits of War,” On the Chinese Revolution in Military Affairs, ed. Shen Weiguang, New China Press, 2004, pp. 105-112.
- [321] Ibid.
- [322] Ibid.

- [323] Ibid.
- [324] Ibid.
- [325] Bates Gill and Lonnie Henley, "China and the Revolution in Military Affairs," 20 May 1996, Strategic Studies Institute, Carlisle Pa., paper downloaded from the Internet on 9 September 2005 at <http://www.fas.org/nuke/guide/china/doctrine/chinarma.pdf>.
- [326] Ibid.
- [327] Dai.
- [328] Wang Baocun.
- [329] Ibid.
- [330] Ibid.
- [331] Ibid.
- [332] Timothy L. Thomas, Dragon Bytes, 2004, Foreign Military Studies Office, pp. 80-96.
- [333] Chinese People's Liberation Army Officer's Handbook, Qingdao Publishing House, June 1991, p. 197. Translation support for the terms science of military stratagem and science of military stratagem was provided by Mr. John Tai, a George Washington University PhD candidate and consultant on Chinese affairs. Dr. Gary Bjorge of the Combat Studies Institute of Fort Leavenworth, Kansas made his PLA Handbook available for use.
- [334] Ibid.
- [335] Niu Li, Li Jiangzhou, and Xu Dehui, "Planning and Application of Strategies of Information Operations in High-Tech Local War," Zhongguo Junshi Kexue (China Military Science), Number 4 2000, pp. 115-122 as translated and downloaded from the FBIS Website on 9 November 2000
- [336] Koh Kok Kiang, and Liu Yi (translators), Secret Art of War: Thirty-Six Stratagems, 1992, Asiapac Books, Singapore, Forward.
- [337] See <http://www.dtic.mil/doctrine/jel/doddict/>, as amended through 17 December 2003.
- [338] Funk and Wagnalls Standard College Dictionary, Harcourt, Brace, and World, 1968, p. 1323.
- [339] Ibid.
- [340] Ibid., p. 1363.
- [341] E-mail correspondence with Dr. William W. Whitson, 13 April 2004. Dr. Whitson is the author of The Chinese High Command, a comprehensive study of China's military elite. He served as a military attaché to Taiwan and Hong Kong, and received his PhD from the Fletcher School of Law and Diplomacy.
- [342] Erya, Beijing: Zhonghua Shuju, 1982, Vol. 1, p. 19a. Footnotes based on e-mail correspondence with Dr. Deborah Porter, University of Washington, 18 April 2004.
- [343] Ibid., p. 52b.
- [344] Ibid., p. 73a.
- [345] E-mail exchange with Dr. Porter, 18 April 2004.
- [346] Zian Ruyi, Command Decision making and Stratagem, Kunlun Publishing House, Beijing 1999, pp. 4-5, 76-87, 92-97 as translated and downloaded from the FBIS Website on 24 April, 2003.
- [347] Jia Fengshan, "Strategists Embrace High-Tech," Jiefangjun Bao (Liberation Army Daily), 9 April 2003 (Internet version), as translated and downloaded from the FBIS Website on 10 April 2003.
- [348] Kang Hengzhen, "The Origin and Development of Asymmetric Strategy," Zhongguo Junshi Kexue (China Military Science), Number 3, 2002, pp. 70-76 as translated and downloaded from the FBIS Website on 6 March 2003.

- [349] Dai Qingmin, "Innovating and Developing Views on Information Operations," *Zhongguo Junshi Kexue (China Military Science)*, Number 4 2000, pp. 72-77 as translated and downloaded from the FBIS Website on 9 November 2000.
- [350] Niu Li, Li Jiangzhou, and Xu Dehui.
- [351] Ibid.
- [352] Ibid.
- [353] China News Agency, <http://www.chinanews.com.cn/n/2003-04-07/26/291859.html>, 7 April 2003.
- [354] Li Nui, Li Jiangzhou, and Xu Dehui.
- [355] Ibid.
- [356] Liu Aimin, "The Characteristics of Informationized War," *Zhongguo Junshi Kexue (China Military Science)*, 1 August 2001, pp. 69-72 as translated and downloaded from the FBIS Website on 20 November 2003.
- [357] Li Nui, Li Jiangzhou, and Xu Dehui. The Chinese use "thought directing" in this article in the way a US analyst would use perception management.
- [358] Ibid.
- [359] Ibid.
- [360] Ibid.
- [361] Ibid.
- [362] Ibid.
- [363] Li Bingyan, "Emphasis on Strategy: Demonstrating the Culture of Eastern Military Studies," *Zhongguo Junshi Kexue (China Military Science)*, 20 October 2002, pp. 80-85 as translated and downloaded from the FBIS Website on 9 January 2003. Li notes that when Westerners consider a problem, they stress "is it a matter of this or of that?" which is helpful in scientific research. Easterners stress "what is this like, and what is that like?" which is helpful in reaching a profound understanding of societal relationships. As a result, research in China into the "cultural genes and methodologies of Chinese military science and strategy" takes into consideration the Yin and Yang (negative and positive), which is said to have originated in the Book of Changes, or I Ching, and the five-elements (water, fire, metal, wood, and earth) theory. In ancient times, odd- and even-numbered changes referred to changes in battle formations, while true and false changes referred to deception methods to set up an enemy for an attack. Each of China's stratagems is based on this doctrine of changes according to Li. The "Yin-Yang and five-elements theory" addresses mutual attraction and the achievement of overall equilibrium and balance through system coordination in addition to the elimination of contradictions.
- [364] Ibid.
- [365] For further discussion of this issue, see Timothy L. Thomas, "Kosovo and the Current Myth of Information Superiority," *Parameters*, Spring 2000, pp. 13-29.
- [366] Niu, Li, and Xu.
- [367] *Information Warfare*.
- [368] Ibid.
- [369] Dai, "Innovating and Developing Views on Information Operations."
- [370] Ibid.
- [371] Ibid.
- [372] Ibid.
- [373] Ibid.
- [374] Ibid. "Soft" means of employment (temporary sabotage or deception) refer to electronic

jamming, computer-virus attacks, network infiltration, carbonized-fiber bombs, virtual reality attacks, psychological attacks and so on. “Hard” means of employment (permanent sabotage, weakening the overall fighting capacity of an enemy) include conventional arms, sabotage attacks with forces, attacks with electromagnetic pulses, attacks with arms carrying direction finders, and so on.

[375] Ibid.

[376] Ibid.

[377] Ibid.

[378] Jia Fengshan, “Strategists Embrace High-Tech.”

[379] Ibid.

[380] Ibid.

[381] Kang Hengzhen.

[382] Ibid.

[383] Ibid.

[384] Hai Lung and Chang Feng, “Chinese Military Studies Information Warfare,” Kuang Chiao Ching, Number 280, 16 January 1996, pp. 22-23 as translated in FBIS-CHI-96-035, 21 February 1996, pp. 33-34.

[385] Jia Xi and Shi Hongju, “Analysis on Key Elements of Knowledge Warfare,” Jiefangjun Bao (Liberation Army Daily) (Internet Version-WWW), 18 September 2000 as translated and downloaded from the FBIS Website on 18 September 2000.

[386] This author reviewed Dai Qingmin’s Direct Information Warfare and credits the content, concepts, and ideas to the book’s author. The content of Dai’s book is reviewed and paraphrased based on translated material. Translation credit belongs to Senior Chief Bart Zobel of the Navy Reserve Navy Information Operations Command. This chapter includes information from Chapter Two, “Click Network Warfare,” pp. 53-154; Chapter Three, “An Informal Discussion of Information Warfare,” pp. 155-253; and Chapter Four, “Integrated Network-Electronic Warfare,” pp. 255-303 of Dai’s book.

[387] Dai Qingmin, Direct Information Warfare, National Defense University Publishing House, 2002, p. 164.

[388] Ibid., p. 198.

[389] Ibid., p. 112.

[390] Ibid., p. 73.

[391] Ibid., p. 121.

[392] Ibid., p. 240.

[393] Ibid.

[394] Ibid., p. 192.

[395] Ibid., p. 108.

[396] Ibid., p. 257.

[397] Ibid., p. 142.

[398] Ibid., p. 124.

[399] Ibid., p. 148.

[400] Ibid., p. 166.

[401] Ibid., p. 196.

[402] Ibid., p. 68.

[403] Ibid., p. 285.

[404] Ibid., p. 171.

[405] Ibid., p. 169.
[406] Ibid., p. 222.
[407] Ibid., p. 248.
[408] Ibid., p. 283.
[409] Ibid., p. 294.
[410] Ibid., p. 207.
[411] Ibid., p. 297.
[412] Ibid., p. 295.
[413] Ibid., p. 121.
[414] Ibid., p. 302.
[415] Ibid., p. 300.
[416] Ibid., p. 301.
[417] Ibid., p. 170.
[418] Ibid., p. 172.
[419] Ibid., p. 173.
[420] Ibid., p. 199.
[421] Ibid., p. 303.
[422] Ibid., p. 194.
[423] Ibid., pp. 284-287.
[424] Ibid., p. 79.
[425] Ibid., p. 110.
[426] Ibid., p. 151.
[427] Ibid., p. 266.
[428] Ibid., p. 58.
[429] Ibid., p. 96.
[430] Ibid., p. 263.
[431] Ibid., p. 59.
[432] Ibid., p. 66.
[433] Ibid., p. 130.
[434] Ibid., p. 133.
[435] Ibid., p. 134.
[436] Ibid., p. 139.
[437] Ibid., p. 153.
[438] Ibid., p. 143.
[439] Ibid., p. 145.
[440] Ibid., p. 153.
[441] Ibid., p. 226.
[442] Ibid., p. 230.
[443] Ibid., p. 278.
[444] Ibid., p. 252.
[445] Ibid., p. 264.
[446] Ibid.
[447] Ibid., p. 283.
[448] Ibid., p. 278.
[449] Ibid., p. 297.
[450] Ibid., p. 161.

- [451] Ibid., pp. 174-178.
- [452] Ibid., p. 182.
- [453] Ibid., p. 187.
- [454] Ibid., p. 210.
- [455] Ibid., p. 249.
- [456] Ibid., p. 196.
- [457] Ibid., p. 191.
- [458] Ibid., p. 250.
- [459] Ibid., p. 140.
- [460] Ibid., p. 201.
- [461] Ibid., p. 300.
- [462] Ibid., pp. 289-292.
- [463] Ibid., p. 96.
- [464] Ibid., p. 79.
- [465] This author reviewed Shen Weiguang's Deciphering Information Security and credits the content, concepts, and ideas to Shen. Translation credit belongs to Senior Chief Bart Zobel of the Navy Reserve Navy Information Operations Command who translated portions of this book.
- [466] Shen Weiguang, Deciphering Information Security, Xinhua Publishing House, July 2003, pp. 26-67.
- [467] Ibid., p. 26.
- [468] Ibid., pp. 28-30.
- [469] Ibid., pp. 30-34.
- [470] Ibid., p. 55. In another place in the text, Shen lists the forms of IW as electronic, network, intelligence, psychological, hacker virtual command and control, and economic warfare. He adds that strategic competition; theoretical threats; potential counterbalances; and media, philosophical, precision, stealth, and firepower warfare are other means worthy of consideration.
- [471] Ibid., pp. 34-35.
- [472] Ibid.
- [473] Ibid., pp. 55-59.
- [474] Ibid., pp. 26-27.
- [475] Ibid., pp. 29-30.
- [476] Ibid., pp. 30-33.
- [477] Ibid., pp. 35-36.
- [478] Ibid.
- [479] Ibid., pp. 36-38.
- [480] Ibid., pp. 39-40.
- [481] Ibid., pp. 59-60.
- [482] Ibid., p. 47.
- [483] Ibid., p. 48.
- [484] Ibid., p. 51.
- [485] Ibid., p. 54.
- [486] Ibid., pp. 66-67.
- [487] Ibid., pp. 3-25.
- [488] Ibid., pp. 6-7.
- [489] Ibid., pp. 3-4.
- [490] Ibid., pp. 14-15.

- [491] Ibid., pp. 14-22. The bulleted points 1-9 are taken from those pages.
- [492] Ibid., p. 20.
- [493] Ibid., p. 23.
- [494] Ibid., pp. 127-241.
- [495] Ibid., p. 54.
- [496] Ibid., p. 141.
- [497] Ibid., p. 149.
- [498] Ibid., p. 170.
- [499] Ibid., pp. 164-165.
- [500] Ibid. These charts (six in all) were on pages 198-204 of the text.
- [501] Ibid., pp. 336-359. No further page delineation can be provided for this section and the next two sections. The translation was performed by a private company and they did not provide exact page numbers from the Chinese original.
- [502] Ibid., pp. 360-379. No further page delineation can be provided for this section. The translation was performed by a private company and they did not provide exact page numbers from the Chinese original.
- [503] Ibid., pp. 380-405. No further page delineation can be provided for this section. The translation was performed by a private company and they did not provide exact page numbers from the Chinese original.
- [504] This author reviewed Chief Editor Wong Zieh Deh's An Interpretation of Network Centric Warfare and credits the content, concepts, and ideas to Editor Wong and authors of the individual chapters. Translation credit belongs to Senior Chief Bart Zobel of the Navy Reserve Navy Information Operations Command who translated this book.
- [505] Wong Zieh Deh, editor, An Interpretation of Network Centric Warfare, National Defense Industry Press, Beijing, 2004, pp. v-vi.
- [506] Ibid.
- [507] Ibid.
- [508] Ibid., pp. 70-71.
- [509] Bai Jianlin, Zhang Pingding, and Liu Peng, "Expert System for C4KISR System Decision," Xiandai Fangyu Jishu (Modern Defense Technology), Beijing, 1 October 2005 as translated and downloaded from the Open Source Center website on 1 February 2007.
- [510] Wong, pp. 72-75.
- [511] Ibid., pp. 76-77.
- [512] Ibid., pp. 78-79.
- [513] Ibid., p. 80.
- [514] Ibid.
- [515] Ibid., pp. 81-82.
- [516] Ibid., pp. 86-89.
- [517] Ibid., p. 230.
- [518] Ibid., p. 231.
- [519] Ibid., pp. 234-238.
- [520] Ibid., pp. 288-290.
- [521] Ibid., pp. 291-292.
- [522] Ibid., pp. 293-294.

- [523] Ibid., pp. 296-297.
- [524] Ibid., pp. 298-299.
- [525] Ibid., pp. 300-301.
- [526] Ibid., pp. 302-303.
- [527] Ibid., pp. 302-306.
- [528] Ibid., p. 326.
- [529] Ibid., p. 315.
- [530] Ibid., pp. 316-319.
- [531] Ibid., pp. 322-325.
- [532] Ibid., pp. 328-329.
- [533] Ibid., pp. 329-332.
- [534] Ibid.
- [535] Ibid., pp. 333-334.
- [536] Ibid., pp. 335-337.
- [537] Ibid., p. 338.
- [538] Ibid., p. 339.
- [539] This author reviewed the Table of Contents and selected terms from Editor Xu Genchu and Director Dai Qingmin's Study Guide for Information Operations Theory. Translation support was provided by a private company.
- [540] Xu Genchu and Dai Qingmin, Study Guide for Information Operations Theory, Academy of Military Science Press, November 2005, pp. 1-3. All of the information that follows in this chapter are short summaries of selected sections taken from this work. The footnote after each section heading indicates the pages from which the information was taken.
- [541] Ibid.
- [542] For a description of informatized operations, see question 54 below.
- [543] Xu and Dai, pp. 1-3.
- [544] Ibid.
- [545] Ibid., pp. 29-30.
- [546] Ibid., pp. 39-40.
- [547] Ibid., pp. 45-46.
- [548] Ibid., p. 48.
- [549] Ibid., pp. 51-52.
- [550] Ibid., p. 52.
- [551] Ibid., pp. 55-57.
- [552] Ibid., pp. 57-58.
- [553] Ibid., pp. 58-60.
- [554] Ibid., pp. 62-64.
- [555] Actual strategies not listed in the book.
- [556] Xu and Dai, pp. 68-69. For questions 52 and 53 (IW and IO), near exact translations from Study Guide for Information Operations Theory are used.
- [557] Ibid.
- [558] Ibid.
- [559] Ibid., pp. 91-92.
- [560] Ibid., pp. 70-71.
- [561] Ibid., pp. 71-73.
- [562] Ibid., pp. 73-74.

[563] Ibid., pp. 74-76.
[564] Ibid., pp. 80-81.
[565] Ibid., p. 81.
[566] Ibid., p. 82.
[567] Ibid.
[568] Ibid., pp. 82-83.
[569] Ibid., p. 83.
[570] Ibid., pp. 84-85.
[571] Ibid., pp. 85-87.
[572] Ibid., pp. 87-88.
[573] Ibid., pp. 88-90.
[574] Ibid., pp. 90-91.
[575] Ibid., p. 91.
[576] Ibid., pp. 91-92.
[577] Ibid., pp. 93-94.
[578] Ibid., pp. 93-94.
[579] Ibid., pp. 94-95.
[580] Ibid., p. 95.
[581] Ibid., p. 96.
[582] Ibid., pp. 96-97.
[583] Ibid., pp. 97-98.
[584] Ibid., pp. 98-99.
[585] Ibid., pp. 111-112.
[586] Ibid., pp. 113-115.
[587] Ibid., pp. 115-117.
[588] Ibid., pp. 117-119.
[589] Ibid., pp. 119-121.
[590] Ibid., pp. 121-122.
[591] Ibid., pp. 145-146.
[592] Ibid., pp. 154-156.
[593] Ibid., pp. 161-162.
[594] Ibid., pp. 164-168.
[595] Ibid., pp. 168-170.
[596] Ibid., pp. 171-173.
[597] Ibid., p. 186.
[598] Ibid., pp. 186-187.
[599] Ibid., pp. 195-196.
[600] Ibid., pp. 202-203.
[601] Ibid., pp. 203-204.
[602] Ibid., pp. 205-206.
[603] Ibid., pp. 206-207.
[604] Ibid., pp. 209-210.
[605] Ibid., pp. 210-211.
[606] Ibid., pp. 211-213.
[607] Ibid., pp. 294-295.
[608] Ibid., pp. 314-316.

- [609] Ibid., pp. 317-318.
- [610] Ibid., pp. 318-319.
- [611] Ibid., p. 392.
- [612] Ibid., p. 395-396.
- [613] Ibid., pp. 396-399.
- [614] Ibid., pp. 400-401.
- [615] Ibid., pp. 403-404.
- [616] Ibid., pp. 404-405.
- [617] Ibid., pp. 405-406.
- [618] Ibid., pp. 406-407.
- [619] Ibid., pp. 407-408.
- [620] Ibid., pp. 408-409.
- [621] This author reviewed editor Yao Youzhi's Warfare Strategy Theory and credits the content, concepts, and ideas to the book's editor and the authors of the individual chapters. The content of Yao's book is reviewed and paraphrased based on translated material. Translation credit belongs to Senior Chief Bart Zobel of the Navy Reserve Navy Information Operations Command who translated portions of the text.
- [622] Yao Youzhi, Editor-in-Chief, Warfare Strategy Theory, Liberation Army Press, 2005, p. 349.
- [623] Ibid., p. 328.
- [624] Ibid.
- [625] Ibid., pp. 328-329.
- [626] Ibid., pp. 330-331.
- [627] Ibid., pp. 331-333.
- [628] Ibid., pp. 334-337.
- [629] Ibid., p. 338.
- [630] Ibid., pp. 339-340.
- [631] Ibid., pp. 341-345.
- [632] Ibid., pp. 346-349.
- [633] Ibid., pp. 99-101.
- [634] Ibid., pp. 153-156.
- [635] Ibid., pp. 215-219.
- [636] Ibid.
- [637] Ibid., pp. 226-229.
- [638] Ibid.
- [639] Ibid.
- [640] Ibid.
- [641] Ibid., pp. 469-472.
- [642] Ibid., pp. 475-476.
- [643] Ibid., pp. 477-481.
- [644] Ibid.
- [645] Ibid.
- [646] Kang Hengzhen, "The Origin and Development of Asymmetric Strategy," China Military Science, No 3, 2002, pp. 70-76 as translated and downloaded from the FBIS website on 6 March 2003.
- [647] Warfare Strategy Theory, pp. 253-256.
- [648] Ibid.

- [649] Ibid.
- [650] Ibid.
- [651] Ibid., pp. 257-259.
- [652] Ibid., pp. 259-261.
- [653] Ibid., pp. 261-265.
- [654] Ibid., pp. 265-267.
- [655] Ibid., pp. 577-580.
- [656] Merriam-Webster's Collegiate Dictionary, Tenth Edition, Merriam-Webster, Inc., 1998, p. 299.
- [657] China's White Paper on National Defense 2006, Beijing Xinhua Domestic Service, 29 December 2006, as translated and downloaded from the Open Source Center website on 31 December 2006.
- [658] Ibid., p. 150.
- [659] Ibid., pp. 138-143.
- [660] Ibid.
- [661] Peng Guangqian and Yao Youzhi, editors, The Science of Military Strategy, Military Science Publishing House, Beijing, English Edition, 2005, pp. 132-133.
- [662] Ibid., p. 39.
- [663] Ibid., p. 57. The three stages of protracted war were listed as the enemy's strategic offense and friendly strategic defense, the enemy's strategic consolidation and friendly preparation for the counteroffensive, and friendly counteroffensive and the enemy's strategic retreat.
- [664] Peng and Yao, pp. 53-55.
- [665] Ibid., pp. 62-72.
- [666] Ibid., p. 9.
- [667] Ibid., pp. 266-267.
- [668] Ibid., p. 381.
- [669] Chinese Military Encyclopedia, Academy of Military Science Press, Volume 3, July 1997, p. 699.
- [670] Dai Qingmin, Direct Information War, National Defense University Publishing House, 2002, p. 108.
- [671] Xu Genchu and Dai Qingmin, Study Guide for Information Operations Theory, Academy of Military Science Press, November 2005, pp. 68-69.
- [672] Tan Haitao and Yang Jie, "Information Warfare," Chinese Military Encyclopedia, Military Science Publishing House 2002, pp. 527-528.
- [673] Direct Information War, p. 279.
- [674] Study Guide for Information Operations Theory, pp. 70-71.
- [675] Ibid.
- [676] The concept of control was covered quite extensively in Dragon Bytes and in Yao's book Warfare Strategy Theory (Chapter 34).
- [677] Peng and Yao, p. 231.
- [678] Deciphering Information Security, pp. 26-67.
- [679] Direct Information War, pp. 292-297.
- [680] Peng and Yao, p. 317.
- [681] Ibid., pp. 397-398.
- [682] Wang Ling, "Comparative Studies of the Comprehensive Power of Major World Countries," 2006: World Political and Security Report (Yellow Book of International Politics), Li Zhenming

and Wang Yizhou, editors, Social Sciences Academic Press, p. 240.

[683] Ibid., p. 267.

[684] Ibid.

[685] Loretta Chao, "Cellphone Ads are Easier Pitch in China," The Wall Street Journal, 4 January 2007, p. B5.

[686] Peng and Yao., p. 406.

[687] Ibid., p. 342.

[688] Ibid., p. 344.

[689] Ibid., pp. 340-343.

[690] China's White Paper on National Defense 2006, Beijing Xinhua Domestic Service, 29 December 2006, as translated and downloaded from the Open Source Center website on 31 December 2006.

[691] Direct Information Warfare, pp. 219-220.

[692] Peng and Yao, pp. 418-419.

[693] Ibid., p. 345.

[694] Ibid.

[695] Ibid.

[696] Direct Information War, p. 170.

[697] Ibid., p. 169.

[698] Ibid.

[699] Peng and Yao, p. 428.

[700] Ibid., p. 154.

[701] Ibid., pp. 206, 222.

[702] Ibid., pp. 142-143.

[703] Ibid., p. 58.

[704] Ibid., pp. 75-76.

[705] Ibid., pp. 272-274.

[706] Ibid.

[707] Ibid., p. 296.

[708] Ibid., pp. 257-261.

[709] Ibid., pp. 153-156.

[710] Peng and Yao, p. 213.

[711] Ibid., p. 215.

[712] Ibid., p. 287.

[713] Ibid., p. 404.

[714] Senior Chief Bart Zobel of the Navy Reserve Navy Information Operations Command translated the entries in this Appendix.

[715] Tan Haitao and Yang Jie, "Information Warfare," Chinese Military Encyclopedia, Military Science Publishing House 2002, pp. 527-528.

[716] Su Jianzhi, "Information Warfare Technology," Chinese Military Encyclopedia, Military Science Publishing House, 2002, p. 528. This section was translated by Senior Chief Bart Zobel of the Navy Reserve Navy Information Operations Command.

[717] Chen Yongguang, "Operations Research and Analysis of Information Warfare," Chinese Military Encyclopedia, Military Science Publishing House, 2002, pp. 528-529. This section was translated by Senior Chief Bart Zobel of the Navy Reserve Navy Information Operations Command.

[718] The author would like to thank Senior Chief Bart Zobel for translating all of the articles used in this chapter from the Sixth International Seminar on Sun Tzu's Art of War.

[719] Hao Yinglu and Zhao Xiaomin, "A Few Issues Concerning Sun Tzu's Art of War and Strategic Psychological Warfare," paper for the Sixth International Seminar on Sun Tzu's Art of War, November 2004. All Chinese comments in this section are taken from this paper.

[720] Zhou Min, "The Basis for the Psychological Warfare Planning of Sun Tzu," paper from the Sixth International Seminar on Sun Tzu's Art of War," November 2004. All material in this section is credited to Zhou.

[721] Ai Songru, "Sun Tzu's Ideas on Psychological Warfare and Their Direction in Modern Psychological Warfare," paper from the Sixth International Seminar on SunTzu's Art of War, November 2004. All information in this section is credited to Ai.

[722] Jiang Lei, "Sun Tzu's Thoughts on War and Reflections on Informationized War," paper from the Sixth International Seminar on Sun Tzu's Art of War," November 2004. All information in this section is credited to Jiang.

[723] Chai Yuqiu, "Sun Tzu's Strategic Thought and Its Inspiration for Informationized Warfare," paper from the Sixth International Seminar on Sun Tzu's Art of War, November 2004. Credit for all information in this section belongs to Chai.

[724] Yu Jinag and Xiong Yuxiang, "Enhancing Psychological Warfare Capability by Learning from Sun Tzu's Military Thoughts"; Zhang Zhiping, "Sun Tzu's Thought of 'Subduing' and Aerospace Power in the Information Age"; and Wang Huqiang, "Sun Tzu's Idea of 'Deception' and Information War," papers from the Sixth International Seminar on Sun Tzu's Art of War. Only abstracts of these presentations were available.

[725] Zhang Zuiliang, et. al., Military Operational Research, Beijing: Military Science Press, 1993, p. 203.

[726] See [US] United States Department of Defense: "Network-centered Combat – Report of the United States Department of Defense to the State Department," Translation of the Chinese Center for Defense Science and Technology Information, Beijing: Chinese Center for Defense Science and Technology Information, 2002, pp. 3-4.

[727] Zhang Zuiliang, et. al., pp. 131-134.

[728] [US] T. N. DuBois: "Grasping War – Military History and War Theory," Translation of the Military Science Institute Foreign Military Research Department, Beijing: Military Science Press, 1993, p. 87.

[729] Ibid., p. 97.

[730] Ibid, pp. 90-91.

[731] Ibid, p. 95.

[732] Zhang Zuiliang, et al., pp. 116-117.

[733] Xu Xuewen, Wang Shouyun, Modern War Models, Beijing: Science Publishing House, 2001, p. 91.

[734] [US] United States Department of Defense, "Network-centered Combat – Report of the United States Department of Defense to the State Department," Translation of the Chinese Center for Defense Science and Technology Information, Beijing: Chinese Center for Defense Science and Technology Information, 2002, p. 48.

[735] [US] Douglass C. North: "System, System Changes, and Economic Achievements," Liurui

Huashi, Taiwan: Times Cultural Press, 1994, p. 113.

Table of Contents

FOREWORD	4
INTRODUCTION	5
CHAPTER ONE: THE SCIENCE OF MILITARY STRATEGY	12
Introduction	12
Understanding the Chinese Concept of Strategy	14
Official Definitions	14
Factors Affecting Strategy: Chinese Views	15
Factors Affecting Strategy: US Views	16
The Science of Strategy	17
Basic Theory of Strategy: Basis of the Science of Strategy	18
General: Primary Divisions of Strategy's Basic Theory	18
Concept of Strategy	19
Related Elements of Strategy	19
History and the Evolution of the Laws of Strategic Theory	20
Laws of Strategic Thinking	21
Chinese Methods of Strategic Studies	23
Applied Theory: General Laws of War and the Conduct of War	23
General: Primary Divisions of Strategy's Applied Theory	23
Strategic Planning: Subset of Strategic Formulation	24
Strategic Guidance for the Employment of Military Force: Subset of Strategic Performance	24
Strategic Information Operations (IO) and Strategic Psychological Warfare (SPW)	24
Local War under High-Tech Conditions	29
Short Summaries of Other Chapters	31
Taiwan	37
Conclusions	38
Postscript	38
Review of the Book's Contents	38
Summary Comparison of Chinese and US Strategic Views	39
CHAPTER TWO: THE SCIENCE OF INFORMATION OPERATIONS	45
Introduction	45
The Science of Information Operations	45
Basic IO Theory	46
Applied IO Theory	48
Technical IO Theory	49
Xu's Recommendations/Conclusions	50
CHAPTER THREE: CHINA'S REVOLUTION IN MILITARY AFFAIRS	

AND INFORMATION OPERATIONS	
Introduction	53
Early Chinese RMA Thoughts	54
China's RMA Theory in 2004: Now with Chinese Characteristics	55
How Do These Experts Define a Revolution in Military Affairs?	58
What Is Strategy?	60
How Does the RMA Impact Strategy?	61
What Is IW, and How Does It Relate to the RMA and Strategy?	62
IW Will Reduce Destruction	63
IW Transforms the Military	64
IW's Technological Impact	64
IW Imparts an Offensive Nature to Modern Conflicts	65
How Did the RMA Influence US Actions in Iraq?	66
What Is Decision Making?	67
Conclusions	67
CHAPTER FOUR: CHINA'S IW-STRATEGY/STRATAGEM LINK	71
Introduction	71
Integrating High-Tech Weaponry with Stratagems	74
Focus on Science and Technology, Not Just Strategy	78
General Dai on IW Strategies	80
Further Thoughts on Stratagems	82
Psychological Manipulation	83
CHAPTER FIVE: DIRECT INFORMATION WARFARE	85
Introduction	85
Defining Terms	85
Direct IW Concepts	87
Information Operations	87
Information Supremacy	90
Networks	91
Network Warfare Units and Personnel	92
Network Psychological Warfare	93
Information Operations Mobilization	94
Integrated Network and Electronic Warfare (INEW)	95
The Commanding Heights of Future War	96
Dai's Recommendations/Conclusions	98
Table of Contents	99
CHAPTER SIX: DECIPHERING INFORMATION SECURITY	102
Introduction	102
10 July 2002, Baoguo Temple, Beijing[466]	102

10 July 2002, Baoguo Temple, Beijing[466]	102
August 2002, Baoguo Temple, Beijing[487]	106
The Information Security University[494]	108
Teaching Plans/Course Outlines for Military Information Security Studies[500]	109
16 April 2003, Chengdu Command[501]	117
June 2003 Interview in Warrior News[502]	118
28 May 2002, Armed Police Forces[503]	119
Table of Contents	120
CHAPTER SEVEN: AN INTERPRETATION OF NETWORK CENTRIC WARFARE	122
Introduction	122
The C4ISR System of Network Centric Warfare	123
Integrated Weapons in Network Centric Warfare	125
Battlefield Management in Network Centric Warfare	126
Meeting Challenges and Achieving Leapfrog-style Development	128
Table of Contents	129
CHAPTER EIGHT: STUDY GUIDE FOR IO THEORY	136
Introduction	136
Informationization	138
The New Revolution in Military Affairs	139
Information Warfare, Informatized Operations, and Informatized War	144
The Characteristics, Rules, and Principles of Informatized War	158
Information Technology	164
Informationized Armed Forces	168
Informationization of the Armed Forces	170
Battlefield Information Systems	174
Informationized Operations Command	174
Joint Operations	177
Table of Contents	182
CHAPTER NINE: WARFARE STRATEGY THEORY	200
Introduction	200
Informationized Warfare	200
Associated Informationized Aspects of Warfare Strategy Theory	203
Asymmetric Warfare	206
Conclusions	208
Table of Contents	209
CHAPTER TEN: CONCLUSIONS	216
Introduction	216
Exploring Components of the Strategy-IO Relationship	217

The Theme of Collecting Technical Parameters and Preemption	226
1999-2003 Books	228
2004-2006 Books	229
Final Thoughts	232
APPENDIX ONE: IW ARTICLES IN CHINA MILITARY SCIENCE: 2004-2006	236
APPENDIX TWO: IW DEFINITIONS IN THE CHINESE MILITARY ENCYCLOPEDIA[714]	240
Brief History	241
Characteristics	242
Forms	243
Looking Ahead	244
Forms and Development	246
Research Content and Methods	246
Development Trends	247
APPENDIX THREE: SUN TZU ART OF WAR CONFERENCES AND IW SUBJECTS[718]	248
A Few Issues Concerning Sun Tzu’s Art of War and Strategic Psychological Warfare[719]	248
The Basis for the Psychological Warfare Planning of Sun Tzu[720]	250
Sun Tzu’s Ideas on Psychological Warfare and Their Direction in Modern Psychological Warfare[721]	250
Sun Tzu’s Thoughts on War and Reflections on Informationized War[722]	253
Sun Tzu’s Strategic Thought and Its Inspiration for Informationized Warfare[723]	253
Abstracts of a Few Papers Not Issued[724]	255
APPENDIX FOUR: DISCUSSION OF THE FORMS OF INFORMATION WARFARE	256
IV. A Dynamics Equation for Military Combat Strength “Quantization”	256
1. Combat Strength Quantum Mathematical Model	256
2. Mathematical Model for Information Structural Strength	259
3. Formula for Calculation of Troop Combat Strength under Different Media Systems	260
4. A Variable Structure Mathematical Model for the Combat Strength System of an Informationized Army	262
DEDICATION	268
ACKNOWLEDGEMENT	269
NOTES	270