THIS FILE IS MADE AVAILABLE THROUGH THE DECLASSIFICATION EFFORTS AND RESEARCH OF:

THE BLACK VAULT

THE BLACK VAULT IS THE LARGEST ONLINE FREEDOM OF INFORMATION ACT / GOVERNMENT RECORD CLEARING HOUSE IN THE WORLD. THE RESEARCH EFFORTS HERE ARE RESPONSIBLE FOR THE DECLASSIFICATION OF THOUSANDS OF DOCUMENTS THROUGHOUT THE U.S. GOVERNMENT, AND ALL CAN BE DOWNLOADED BY VISITING:

HTTP://WWW.BLACKVAULT.COM

YOU ARE ENCOURAGED TO FORWARD THIS DOCUMENT TO YOUR FRIENDS, BUT PLEASE KEEP THIS IDENTIFYING IMAGE AT THE TOP OF THE .PDF SO OTHERS CAN DOWNLOAD MORE!

UNCLASSIFIED

THEMES IN CHINESE WRITINGS ON INFORMATION WARFARE, 1995-1999

FINAL REPORT

BY
MICHAEL BROWN
ANDREW MAY

REPORT PREPARED FOR THE OFFICE OF NET ASSESSMENT,
OFFICE OF THE SECRETARY OF DEFENSE
CONTRACT NO. DASW01-95-D-0060, D.O. 56
SAIC PROJECT NO. 01-1175-04-1299-000
DOCUMENT NO. SAIC-00-6959+SAC
COMPLETED MARCH 10, 2000

The Strategic Assessment Center
Science Applications International Corporation
1710 Goodridge Drive, McLean, VA 22102

20061003247

UNCLASSIFIED

DESTRUCTION NOTICE - For classified documents, follow the procedures in DOD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM), Chapter 5, Section 7, or DOD 5200.1-R, Information Security Program Regulation, Chapter IX. For unclassified, limited documents, destroy by any method that will prevent disclosure of contents or reconstruction of the document.

OSD/NA

Distribution B: Distribution authorized to U.S. Government agencies only due to Proprietary Information, (3/1999). Other requests for this document shall be referred to Office Secretary of the Secretary of Defense, Office of Net Assessments (OSD/NA). 1920 Defense Pentagon. Washington. DC 20301-1920.

THEMES IN CHINESE WRITINGS ON INFORMATION WARFARE, 1995-1999

FINAL REPORT

CONTENTS

THEMES IN CHINESE WRITINGS ON INFORMATION WARFARE, 1995-1999

EXECUTIVE SUMMARY

Chinese defense analysts have demonstrated, over the past several years, a growing interest in the tools and techniques of information warfare. The purpose of this report is to analyze unclassified articles appearing in the Chinese press between 1995 and 1999, with a particular intent to determine what themes – ideas, concerns, and underlying assumptions – appear and re-appear throughout the literature.

Our analysis and conclusions are detailed in the report. In short form, we found that:

- There appeared to be no agreed analytical framework for debate on information operations or information warfare, and there was no evidence of a consensus definition of what does and does not constitute information warfare. In the absence of such a framework, Chinese discussions of IW tended to be diffuse and were often lacking in analytical rigor.

- Many of the articles appear intended not to further debate but rather simply to educate young officers, non-commissioned officers, and PLA soldiers, and introduce them to notions of high-tech warfare, particularly information warfare.

- Throughout the period we examined, the Chinese were inclined to view the United States as both a competitor to frustrate and a model to emulate. Most Chinese IW analysts seemed torn between a desire to develop forces like the U.S. military's and the recognition that such forces are far out of reach, making low-tech "asymmetric" capabilities a wiser investment. In either case, the U.S. stands out as the one nation on which virtually all analysis was focused.

- Chinese analysts focused on using IW and IO at the operational and tactical levels of warfare, giving comparatively little thought to either strategic information warfare or defensive IW measures. In 1999, we did uncover a trend toward greater consideration of both strategic and defensive IW: it remains to be seen whether this is an aberration brought on by external events or the beginning of a real shift in Chinese thinking.

- When discussing IW, Chinese analysts tended to consider it as a complement to so-called "hard attacks" (i.e., physical destruction). Specifically, most analysts look upon IW as particularly well-suited to the initial phases of warfare and a preferred means of seizing the initiative. There is little evidence of belief that IW alone could achieve effects comparable to more conventional "hard" weapons.

- When examining U.S. actions in recent conflicts (the Gulf War and the conflict over Kosovo), Chinese analysts tended to focus on America's adversary, and appear to be particularly interested in low-tech countermeasures that might be employed to offset America's overwhelming technological advantage.

- There is much discussion, at present, about how China ought to proceed in modernizing its forces, personnel, and military organizations. Much of this debate has centered on the critical roles of theory, training, and organizational change, though there is little evidence, as of yet, of serious change being implemented. There is also some question as to how aggressively China ought to pursue modernization. Three models seem most popular: stages (gradual, planned change); transcendental (leapfrogging to RMA forces); and comprehensive (hedging with both gradual modernization and rapid advance). It seemed clear, from the literature we reviewed, that China has yet to determine which sort of path to pursue.

I. Introduction

Between 1993 and 1999, there were an increasing number of articles appearing in the Chinese press on Information Warfare and Information Operations. In the earlier years (1993 and 1994), these articles focused primarily on developments in the West, and on topics that were interesting – but of minimal military value – like the use of malicious code for specific purposes. Over the years, however, Chinese thinking appears to have developed significantly. To analyze this development in somewhat more detail, in early 1999 the Director of the Office of Net Assessment, Office of the Secretary of Defense, requested that the Strategic Assessment Center, SAIC, undertake a study of trends in Chinese writings on information warfare and information operations, focusing on unclassified writings in the 1995-1999 time frame. The objective of this effort was to identify the trends in Chinese thought on IO/IW over the past five years. The study was to be focused on the following questions:

- What are the trends in Chinese thinking on IO and IW?
- What is the rationale underlying these trends?
- How confident can we be that these are underlying trends?

In accomplishing this task, we drew most heavily upon the unclassified primary sources made available through the Foreign Broadcast Information Service (FBIS), conversations with other experts, and a few secondary sources. This report presents our findings: the Introduction sets out the terms of our study and explains the format of the paper, while the second section outlines the general approach we have taken. The third section, "Context," examines the broader strategic and political backdrop against which discussions of information warfare have taken place in China. The fourth section, "Observations," is the bulk of the report, and presents what we found to be the salient themes in the unclassified Chinese writings we examined. A fifth section presents our conclusions, and a sixth and final section offers a few insights into possible implications for the Department of Defense. We have also included, as appendices, translations of a few of the articles we found most interesting.

II. Approach

We approached this study not as experts in Chinese strategic thought or Chinese culture, but as analysts who have been studying the military and strategic dimensions of information warfare – at least as it has developed in the United States – over the past five years. Our approach is based on our understanding of how American thinking on this topic has evolved over time, what the prevailing notions are today, and what, in some sense, constitutes reasonably sophisticated thinking about information warfare.

We recognize fully the limitations of this approach. First, written sources reveal only certain perspectives. Areas on which there is universal agreement, for example, tend not to receive a great deal of attention, and accepted truths are rarely addressed explicitly. Further, particularly on a subject like information warfare, it is rare to find non-believers, or even skeptics, participating in the written debate. While we cannot eliminate this potential shortcoming, we can mitigate its impact. By reading a great deal of material and analyzing it closely, we believe we can identify the kinds of accepted truths and implicit assumptions that undergird this body of writing, and by placing our discussion in the broader context of strategic debate in China, we can avoid the implication that all Chinese defense analysts are IW enthusiasts.

Second, we recognize that by relying on translated documents we are examining a biased set of Chinese writings. It is biased both because the documents upon which they translations are based are public and unclassified, and because the Foreign Broadcast Information Service (FBIS) – upon which we relied extensively – can translate only a small portion of the vast number of open source documents on Information Warfare. FBIS tends to focus their efforts on translating a broad range of articles, which can be valuable but tends to complicate identification of trends. To ensure our sample of writings is not *too* biased, we read secondary sources in English and discussed our findings with Chinese language specialists to determine where and how our findings might be different from theirs. Finally, and perhaps most important, we can remember that our intent is to focus on *how* the Chinese are thinking about the problem – not on specific steps they are taking or capabilities they are developing. This, we believe, can be determined through the unclassified literature.

Finally, we recognize that five years may simply be too short a time to establish definitive "trends," particularly for a topic that is still in the very early stages of development. As a result, we determined to focus on emerging *themes* –ideas, concerns, or underlying assumptions that tended to appear and re-appear in the literature. Some of these themes were constant throughout the period; others changed over time.

In sum, we feel there is much to recommend the approach that we have taken. There is value, we believe, in having another perspective on the issue to determine if those whose expertise lies in the evolution of U.S. Information Warfare doctrine is similar to those whose specialty is China or Chinese strategic thought. We believe that this approach makes particular sense with respect to information warfare: as we will show, Chinese writings on information warfare appear to be largely derivative of U.S. analyses, meaning that cultural or broad strategic factors may have somewhat less influence in shaping Chinese thinking about IW (at least in this stage of development) than they usually do. An understanding of U.S. theories, in short, may shed valuable light on the evolution of Chinese thinking about information warfare.

III. Context

One of the reasons that examining themes in the Chinese Information Warfare/Information Operations literature is difficult is that China is in the midst of a strategic transition, not only with regard to the importance of information and other technologies, but also with respect to the role Beijing wants to play in regional and international security. Mainstream Western analysts and a number of Chinese scholars argue that this transition can be captured in the change in strategic focus from "early war, major war and nuclear war," to what has been termed "local war under high tech conditions." The view has been expressed well by Li Nan. He argues that the emerging doctrine is based on the increasingly widespread belief in the Chinese military that future warfare will be characterized by surprise attacks, quick resolution, greater reliance on elite troops, deep strikes, and high-tech conventional weapons.[1] Michael Pillsbury, however, in his analysis of Chinese strategic thought, takes issues with this approach and cautions that the reality may be more complicated. He suggests that there is wide-ranging debate taking place within the strategic community, a debate that can best be understood as occurring among three principal schools of thought. The People's War School takes a fairly traditional view, derived from Mao, that war will consist of a years-long, large-scale campaign between China and another major power. The Local War School – supporters of "local war under high-tech conditions" – generally holds that war will be rapidly fought with elite troops and high-tech weaponry (it is this school upon which Li Nan, and many other analysts, have focused almost exclusively). The third school, says Pillsbury, consists of the RMA advocates, those who argue that future warfare will be waged with networked forces, highly reliant on advanced C4ISR, employing directed energy weapons, computer viruses, and anti-satellite attacks.[2] Whether Pillsbury is correct in his

[1] Li Nan, "The PLA's Evolving Warfighting Doctrine, Strategy and Tactics, 1985-95: A Chinese Perspective," *China Quarterly* 146 (June 1996), 179-199.

[2] Michael Pillsbury, "China and the Revolution in Military Affairs," 4-7. See also his monographs, *Chinese Views of Future Warfare* (Washington, DC: National Defense University Press, 1997) and China Debates the Future Security Environment (Washington, DC: National Defense University Press, 2000).

characterization of three schools of thought is less important than the broader point he makes that this is a time of a wide-ranging strategic debate in China. As we examine Chinese writings on information warfare, it is useful to bear in mind the real and pervasive divides characterizing Chinese strategic thought on a spectrum of strategic issues – not just information warfare.

As our brief summary of Pillsbury's work indicates, part of the ongoing debate within China has centered on the possibility of a Revolution in Military Affairs and an attempt to determine what, if anything, such an RMA would mean for China's military forces. Although Chinese thinkers appear no more unified than their American counterparts in their vision of what the RMA will ultimately look like and what it will mean for future warfare, there is a baseline of agreement – among those who believe that an RMA is underway – about the general characteristics of this revolution in military affairs. The building consensus appears to be that the RMA will have five dimensions: ground, sea, air, space, and electromagnetic. This is somewhat surprising in that among U.S. analysts of the RMA there is no comparable consensus on the "dimensions" of future warfare. There are differences of opinion, for example, on whether "air" and "space" are separate dimensions of warfare or one; and differences on whether "electromagnetic," "information" or "knowledge" should be the focus of a new area of warfare. Indeed, some American analysts are not convinced that "dimensions" are a useful construct for thinking about future warfare. What we find surprising is the degree to which Chinese RMA analysts appear to accept the utility of "dimensions" *and* tend to cite the same dimensions over and over.

Chinese authors also appear to be in general agreement that in the future ground warfare will have a greatly increased battlespace, will have no "fronts" as we understand them, and will take place at a much higher tempo than it does today. Conflict at sea, most believe, will be characterized by emphasis on undersea warfare; air power will be long-range, stealthy, and linked to space; and space warfare itself will be critical to victory and will focus largely on C3I.[3] One of the most interesting elements of this is the focus on electromagnetic warfare: this broad area includes information operations, information warfare, and weapons such as HERF guns and much-discussed "virus guns," which some authors appear to believe to be capable of remotely inserting viruses into computers via electromagnetic transmissions.[4] Most Chinese analysts are quick to point out that the RMA is far from complete; that the demonstrations of U.S. military might in the Gulf War and Kosovo reflect not a completed revolution but a revolution in progress.

It should be emphasized that Chinese writings on future warfare in general and the RMA in particular are infused with at least partial recognition of just how far behind China currently lags, especially with respect to high-technology weaponry. Chinese analysts frequently cite their nation's developing economy, limited technical base, and underdeveloped educational system as factors impeding their defense modernization. There is as well a widespread sense that the current RMA offers tremendous opportunities for nations such as China that currently lag behind to make significant progress toward achieving substantial military capability. As will be discussed, this recognition of technological backwardness has strongly influenced the ways in which Chinese analysts view the prospects for information warfare and, more broadly, the possible emerging U.S.-China competition. Thus, the Chinese appear, from these writings, to be a nation that believes it lags well behind in critical technologies but is determined that the

[3] See the articles collected in *Chinese Views of Future Warfare*. A representative view of how information technology will fit in to the larger RMA can be found in Lieutenant General Huai Guomo, "On Meeting the Challenge of the New Military Revolution," *Zhongguo Junshi Kexue* (*China Military Science*) 20 February 1996. There is also evidence of considerable Chinese interest in biotechnology. Particularly in the mid-1990s, Chinese analysts writing about the RMA tended to include biotechnology in laundry lists of key technologies or areas for research.

[4] See Geng Haijun, "All Types of `Computer Warfare Weapons,'" *Jiefangjun Bao*, 20 Aug 1996 p. 6, and Chen Zhaohai, "Computer Warfare Tactics," *Jiefangjun Bao* , 7 July 1998 p. 6.

nascent information-drive RMA will afford an opportunity for the PLA to make considerable strides.

IV. Observations

Who is Writing about IW, and Where

There is something to be learned, we believe, simply by examining the patterns of who is writing about IW, and the sorts of publications in which these writings tend to appear. By a considerable margin, the majority of articles translated by FBIS have appeared in *Jiefangjun Bao* (*Liberation Daily*), the daily paper of the General Political Department of the PLA, and most of these are drawn from a regular column called "Military Forum."[5] Generally speaking, the authors of these articles are either civilians or the paper simply declines to note a military rank.[6] These articles tend to be short (between 1,000 and 2,000 words), broadly-focused, and analytically shallow. There is little effort to explore issues in depth (very rarely, for example, does an author explain in any detail how IW might actually be *employed*, or what China might *do* to place itself in position to exploit U.S. vulnerabilities), and only very rarely does one author contest or even reference the work of another.

There have also been a number of IW-related articles published in more substantive journals, including *Zhongguo Guofang Keji Xinxi* (China Defense Science & Technology Information), *Jisuanji Shijie* (China Computerworld), *Guofang* (National Defense), and *Zhongguo Junshi Kexue* (China Military Science, sponsored by the Academy of Military Sciences). *China Military Science*, which featured the most articles relevant to our study, generally runs articles

[5] In 1995, introducing a "Military Forum" article by Shen Weiguang (one of the deans of China's IW community), a *Jiefangjun Bao* editor wrote that "This paper has published a large number of articles by foreign armies on information warfare, which has attracted the widespread attention of our readers. In the face of new developments in the military revolutionary situation, we can no longer sit and wait, or remain silent! We should boldly plunge into this 'quiet battlefield' and meet the challenge! A new military revolution is bound to produce an impact on traditional training of military officers, army structure, mobilization of logistics forces, operational thinking, and the trend of thought of national defense as a whole. In this regard, our research will be concentrated onto single pages for a period of time. Readers are welcome to participate in the discussion." *Jiefangjun Bao*, 7 November 1995, p. 6.

[6] About 90% of *Jiefangjun Bao* authors have no listed military rank. After discussions with several people, including Dan Beck of the Foreign Systems Research Center, we believe that most authors are either civilians or of

averaging 4,000 to 8,000 words, nearly all of which are written by military officers or government officials. In these journals – particularly *Military Science* – articles tend to be longer, more focused, and more analytically rigorous. In these pieces, authors often advance individual theses or hypotheses and in some cases attempt to place their work in the context of a broader discussion. Interestingly, however, even in these instances very few authors explicitly challenge the ideas or writings of anyone else in the field, and nowhere did we see efforts to delineate "laws of information warfare," such as one might have expected the Soviets to develop.

It is rewarding to consider, briefly, these two types of articles. While the *Liberation Daily* (*Jiefangjun Bao*) articles are generally of low quality and reveal little sense of sophisticated thinking about information warfare, the most interesting thing about them may be that they appear at all. Since the *Liberation Daily* is written primarily for consumption by the literate enlisted and junior officers of the PLA, the "Military Forum" articles on information warfare may be intended mostly to introduce these personnel to the concept of IW, to get lower-level personnel thinking about the issue, and in general to prepare a foundation of personnel who are at least aware of the basic concepts associated with IW/IO. We believe this may be an important observation, particularly when linked with You Ji's hypothesis that elements of the Chinese military are deliberately cultivating younger officers to lead China's RMA efforts in the future.[7]

comparatively low rank. *Jiefangjun Bao* does sometimes make a note of an author's rank, but almost always when the rank is colonel or higher.

[7] You Ji writes, "Looking into the future, they (young advocates of the RMA in China) will increasingly wield more influence within the PLA and even over national politics as a whole. This is partly because they are strategically positioned within PLA headquarters at various levels, with promising career advancement ahead of them. In PLA tertiary institutions, they have been teaching future PLA leaders and forging useful personal networks. More importantly, their views on RMA are based on their understanding of technological developments in the new century and this has won them the firm support of CMC Chairman Hang Zemin who, as a farsighted technocrat, is very enthusiastic about RMA. This has been the fundamental reason for RMA becoming so popular in the PLA, as RMA advocates get better chances of promotion with Jiang's blessing." In "The Revolution in Military Affairs and the Evolution of China's Strategic Thinking." *Contemporary Southeast Asia*, No. 3, Vol. 21, p. 344.

The more substantive articles, particularly those in *Military Science*, appear to be intended for other high-ranking officers and officials. As will be discussed in greater detail later in this section, these articles, much more than those in *Liberation Daily*, discuss how China might actually go about using information warfare techniques to exploit U.S. weaknesses. Taken together, therefore, these two types of article may indicate both an effort to educate lower-ranking personnel and the existence of rather rigorous and serious thought at the higher levels of the Chinese military bureaucracy. We should consider, in the future, ways of learning more about the different perspectives offered by the various journals, the degree to which these journals may represent the views of competing elements of the Chinese bureaucracy, and the role played by these journals in fostering and delineating debate.

China's Perspective on the U.S. and Information Warfare

China's perspective on military developments in United States seemed to change dramatically between 1998 and 1999. To better explore this apparent division in the evolution of Chinese thinking on IO/IW, we have divided this section into two segments. The first addresses the principal themes with regard to the U.S. we identified between 1995 and 1998, while the second focuses on Chinese writings in 1999.

1995-1998: At least for the period 1995-1998, one of the most interesting – and in some ways unexpected – themes to emerge from Chinese writings on information operations and information warfare is the degree to which Chinese analysts looked at the United States as both a competitor to frustrate (perhaps a future enemy to defeat) and a model to emulate. There can be no question that Chinese IW analysts took as their notional enemy the United States: many, if not most, implicitly or explicitly addressed the threat posed by the U.S. and discussions of future information warfare centered around a U.S.-China conflict. Indeed, it is striking just how openly many authors stated their animus toward the U.S. and the extent to which military analysts – at least those writing about IW – ignored all other potential opponents in lieu of the United States.[8]

Balanced against this perspective was general recognition that the United States is, by a wide margin, the global leader in information technology and has led the way in thinking about future warfare. China, by contrast, is still struggling to modernize its military and lacks the developed conceptual framework for understanding future warfare–something Chinese authors have pointed out repeatedly. In some respects, then, Chinese analysts have emphasized the need to replicate American successes, and tended to follow U.S. actions and writings very closely. Particularly in 1995 and 1996, but continuing through the late 1990s, Chinese authors tended to cite U.S. analysts (such as Martin Libicki, General Gordon Sullivan, and particularly Alvin Toffler) when discussing new or potentially controversial issues. This method of substantiating claims correlates to a tendency, often stated explicitly, to look to the United States as a model military force, in terms of technology, weapons systems, and doctrine.[9] The Chinesc have also followed military experiments and actions very closely. A surprising number of authors, for example, called for greater attention to "digitized forces," citing the successful expcrimentation carried out

[8] There has been an increasing tendency, on the part of Chinese analysts, to decry U.S. hegemonic tendencies. Particularly in 1999, a large number of authors have sounded a note of alarm concerning America's ability to exert tremendous influence over international affairs. See for example Qin Zong, "Guard Against New Development of U.S. Hegemonism," *Beijing Qiushi* 12, 16 June 1999, p. 12-15, and a discussion of the Kosovo Crisis among experts and scholars at China's National Defense University, as reported in *Jiefangjun Bao*, 13 April 1999, p. 6.

[9] The recent, much-publicized Chinese book on unrestricted warfare asserts that "There's no getting around the opinions of the Americans when it comes to discussing what means and methods will be used to fight future wars. This is not simply because the U.S. is the latest lord of the mountain in the world. It is more because the opinions of the Americans on this question really are superior compared to the prevailing opinions among the military people of other nations." Qiao Liang and Wang Xiangsui, *Unrestricted Warfare: Assumptions on War and Tactics in the Age of Globalization* (Beijing: PLA Literature Arts Publishing House, February 1999), 34-59. Noted Chinese IW theorist Shen Weiguang, however, has noted with some frustration that his original thinking about future warfare and IW – which he dates to 1985 – far predates any serious American thinking on these topics. See Shen Weiguang, "Focus of Contemporary World Military Revolution – Introduction to Research in Information Warfare," *Jiefangjun Bao*, 7 November 1995, p. 6.

by the U.S. Army.[10] In fact, the Chinese reported on the Army's Advanced Warfighting Experiment with digitized forces carried out at Fort Irwin with far more enthusiasm and less skepticism than did American analysts.

There was also, in these years, a widespread feeling that there were significant advantages to being a technology follower rather than leader, and that the RMA offered a tremendous opportunity for rapid advances in military capability. For example, defense analysts Wang Jianghuai and Lin Dong wrote that "History has indicated that he who sets off first may not necessarily win the trophy and the biggest input may not necessarily bring about the biggest gain. . . . As long as we seize the opportunity and bounce on the springboard of technological revolution, we will be able to greatly narrow the gap between us and the advanced countries."[11] In mid-1996, Su Enze wrote that "the further technology develops, the more easily technology will be caught up with . . . the third world countries can very often find shortcuts for information technology development and attain similar standards within a shorter period of time."[12] These

[10] Li Yinnian and Li Zongjian, "Network: Dominator of Future Battlefield," *Jiefangjun Bao*, 21 July 1998, p. 6; another analyst cites the April 1994 digitized exercise "Desert Mace M," in which the digitized force won decisively. Xu Huabao, "Scanning of High-Technology Battlefield," *Jiefangjun Bao*, 13 January 1998, p. 6. A more detailed discussion of digitized forces and their importance in future warfare comes in Yuan Banggen, "IW, Digital Battlefields," *Zhongguo Junshi Kexue*, 20 February 1999, p. 46-51. Yuan closes his discussion of digitized forces by noting that the concepts he had explored "are basically of the same nature as those which are currently widely adopted by the US army." On the other hand, another analyst, writing in 1995, paid more attention to the potential drawbacks of "digitalized forces," and concluded, due these potential drawbacks and the high cost associated with upgrading forces, "digitalized forces" were likely to be more important for U.S. forces than for the Chinese. Lin Dong, "Applications of Digitalization in Military," *Guofang* (National Defense), 15 November 1995, No. 11, pp. 10-11. Overall, we found that Chinese authors – even those publishing at the unclassified level – seemed to pay a great deal of attention to what Americans were doing and saying. Apart from the examples noted above, we found numerous references to U.S. activities such as Eligible Receiver, the widespread problems caused by the Morris Worm, and so on. Authors also make reference to rather obscure or specialized U.S. publications, including a lengthy translation of passages from the 1998 RAND paper "Strategic Information Warfare Rising." Interestingly, the Chinese seemed inclined to accept as accurate U.S. reports about the success of various exercises.
[11] Wang Jianghuai and Lin Dong, "Viewing Our Army's Quality Building From the Perspective of What Information Warfare Demands," *Jiefangjun Bao*, 3 March 1998, p. 6.
[12] Su Enze, "Logical Concept of Information Warfare," *Jiefangjun Bao*, 11 June 1996, p. 6. Wang Baocun, a noted expert on IW, wrote in 1998 that the "epochal military revolution which is taking place now at the turn of the

and similar comments indicate that some analysts endorsed what might be considered a "symmetric strategy" – that is, China should seek to attain technologies and forces, such as "digitized units," like those being developed by the United States. These comments also indicate that many analysts believe that time is on China's side and that the PRC can well afford to wait to develop new, potentially revolutionary capabilities until others have researched the technical and operational details.

Perhaps because the magnitude of America's military advantage makes emulation appear extremely difficult, however, many Chinese authors looked to IW not as an area in which the U.S. model should be followed, but rather as an aspect of warfare that might prove to be an Achilles' heel for U.S. forces. Representative of this line of analysis is an article by Jia Weidong, which states that America's information advantage "will be a 'two-edged sword.' The side with the marked technical inferiority that is faced with the threat of asymmetrical warfare can still use certain special means to conduct nuclear, biological, and chemical strikes, either destroying the enemy's advanced information network, or striking with modern guerrilla warfare tactics such as 'unconventional warfare' and terrorism."[13] In this sense, some Chinese analysts

century presents a grim challenge to our army. At the same time, it also provides our army with a historic opportunity. . . . The opportunity created by the new military revolution is a chance of a life time." Wang Baocun, "Military Transformation in an Information Era," *Jiefangjun Bao*, 21 April 1998, p. 6.

[13] Jia Weidong, "Asymmetrical War," *Jiefangjun Bao*, 17 April 1999, p. 6. See also Xu Huabao, "Scanning of High-Technology Battlefield," *Jiefangjun Bao* , 13 January 1998, p. 6. Another article states that "In their own words, a highly computerized open society like the United States is extremely vulnerable to electronic attacks from all sides. This is because the U.S. economy, from banks to telephone systems and from power plants to iron and steel works, relies entirely on computer networks. . . . When a country grows increasingly powerful economically and technologically, its international and domestic ties are bound to become more extensive, and it will become increasingly dependent on modern information systems and therefore suffer heavier losses in a computer invasion . . .any successful computer invasion on an information superhighway may endanger the computer network of an entire society and cause huge irretrievable losses in the twinkling of an eye. . . . [T]he United States is more vulnerable to attacks than any other country in the world. What is more, the study of precautions against computer invasion proves to be far more difficult and sophisticated than the study of means of computer invasion." Zhang Shouqi and Sun Xuegui, "Be Vigilant Against 'Pearl Harbor Incident' in Information Age," *Jiefangjun Bao* 14 May 1996.

indicated that the United States illustrates how a country can develop vulnerabilities by becoming overly dependent upon high-tech equipment – risks that China needs to avoid.[14]

As with much of what appears in the unclassified realm, however, it is difficult to determine how much this writing reflects real thinking on the part of Chinese IW theorists and how much is simply repetition and regurgitation of American writing about this potential vulnerability.[15] It is also worth noting that Chinese authors never, in these cases, offer any sort of details – or even fictional scenarios, such as those developed by Charles Dunlap and John Arquilla – about how IW might actually be employed against the United States in some effective manner.

This unusual situation – with China apparently torn between the desire to emulate and the desire to defeat with asymmetric measures – fundamentally shaped the way in which most Chinese analysts approached the topic of information warfare between 1995 and 1998. As will be discussed in greater detail toward the end of the report, this situation also indicates the presence of an unusual dynamic (one that combines leader-follower and measure-countermeasure) that warrants further study and may offer substantial opportunities for shaping behavior.

[14] Shen Weiguang, one of China's most prominent IW theorists, wrote in 1995 that "History has given evidence to the fact when some new technology brings mankind brightness, a shadow is cast simultaneously. Advanced electronic computers and information technology link society and the army to an integrated network; the result is very high efficiency. On the other hand, a society and an army linked to an integrated network are liable to suffer great fragility. . . . Our research in tactics and technological improvement must start from this point and avoid following in other people's footsteps." Shen Weiguang, Focus of Contemporary World Military Revolution – Introduction to Research in Information Warfare," *Jiefangjun Bao*, 7 November 1995, p. 6.

[15] For example, some authors, in noting U.S. vulnerability to IW attack, cite American documents, including one that is apparently the 1996 DSB report on Information Warfare Defense, stating that "[i]nformation advantage has to depend on sophisticated equipment and facilities, and such a massive system is no doubt an important target for the enemy. The U.S. Committee of Defense Science admits that the information infrastructure is 'extremely vulnerable to attack' and has 'become an as yet unrecognized trap in the history of war.'" Zhou Demin, "Dialectic View of Information Advantages and Disadvantages," *Jiefangjun Bao*, 28 April 1998, p. 6.

1999: Chinese writings in 1999 appeared to take on a significantly different tone from those of the preceding years. The conflict over Kosovo, the inadvertent attack on the Chinese embassy in Belgrade, and increasing tensions over Taiwan combined to fuel anti-U.S. sentiment, leading many Chinese authors to castigate the U.S. as a "hegemonic" power acting without regard for other nations. Some Chinese expressed concern that "we cannot exclude the possibility of a FRY-type problem involving China's internal affairs and ethnic conflicts, in which a U.S.-led Western force would interfere in China's internal affairs through means such as armed threats and even military strikes."[16]

With this new tone came a change in the substance of the articles on IW. There were noticeably fewer articles on emulating the U.S. military and more on how to defeat the U.S., exploiting the vulnerabilities that can come with reliance on high-tech systems. For example, in the wake of America's demonstrated reliance on air power, One author argued that China "should place the greatest strategic importance on anti-air raid operations and beef up our preparations in this respect" including "studying the methods of anti-air raid operations, information operations, and the 'three attacks and three defenses' operations under the high-tech condition (i.e., attack on aircraft, missiles, and commanding systems; defense against accurate strikes, information invasion, and reconnaissance infiltration)."[17] As will be discussed later in the report, Chinese military analysts were particularly intrigued by the low-tech countermeasures Serb forces used to lessen the effectiveness of U.S./NATO bombing raids. Whether these articles represent a change Chinese thinking or are simply an aberration arising from the general political situation is, of course, not yet clear. We do believe, however, that is demands continued attention.

[16] Peng Yang: "The Air Force Strengthens Its Armaments on the Southeast Chinese Coast," Hong Kong *Kuang-Chiao Ching*, No 323 16 August 1999, p. 20-23.
[17] Kung Shuang-yin, "Science and Technology Are Most Needed for Strengthening National Strength," Hong Kong *Ta Kung Pao* 21 May 1999, p. A5.

There are two related points worth considering. The first is that, while the emphasis of Chinese analysis changed somewhat, the basic contradiction between emulation and competition was still present: that is, it would be a considerable overstatement to say that Chinese IW analysts no longer expressed interest in the U.S as a model in terms of advanced weapons and doctrine. Rather, there was an increasing tone of hostility – and particularly a view of the U.S. as "hegemonic" – pervading articles written over the last year or so. Second, even as China's view of the U.S. appears to have shifted somewhat, it is worth noting that the United States is still the focus of Chinese writings, particularly about information warfare. In short, whether China is emulating or competing with the U.S., Chinese analysts will look to U.S. actions, writings, and statements as a critical influence over how China ought to think and behave.

The Lack of an Agreed Analytic Framework

It took the United States several years of intellectual and bureaucratic wrangling to develop a consensus on an analytic framework for information warfare and information operations. As it exists today, this framework consists of unclassified definitions of IW and IO, and a set of categories and subcategories of how those notions could be implemented. The Chinese, however, appear to have had even less success. There has not yet been, at the unclassified level at least, any evidence of even a commonly-agreed definition of information warfare. Although an author will, from time to time, offer a definition of sorts it is nearly always derivative of the American definition.[18] As we will discuss later, the absence of a definition is not simply an

[18] Liang Zhenxing, for example, defines information warfare as "the process of maintaining the integrity of one's own information system while crippling or destroying the information systems of the enemy," in "Major Influence on China's Defense Modernization," *Jisuanji Shijie* (China Computerworld) 8 April 1996, No. 14, pp. 123, 125. This definition is repeated in numerous publications. Variations on this theme are also abundant: for example, one article defines IW as "the struggle waged to seize and keep the control over information, in other words, the struggle between belligerent parties to size the initiative in acquiring, controlling, and using information, by capitalizing on and sabotaging the enemy's information resources, information system, and informationized weapon systems, and by utilizing and protecting one's own information resources, information system, and informationized weapon systems." Untitled article by Yuan Banggen, *Junshi Kexue* (Military Defense), 20 February 1996, pp. 46-51. Although countless variations on this theme are available, the definitions are all similarly vague, and the

academic issue, but seems to manifest itself in that different authors have very different notions of information, information *in* warfare and information warfare itself. As a result of this apparent confusion, many authors appear to be talking past one another.

The Chinese have had the same problem in developing subcategories of information warfare and information operations. Although some authors have attempted to identify subcategories– such as command-and-control warfare, or electronic warfare (both derivative of U.S. writings) –truly systematic efforts are rare and none appear to have been widely accepted. Perhaps the most developed attempt at categorization comes from Wang Baocun, a Senior Colonel and Research Fellow at China's Academy of Military Sciences, who divided information warfare into ten subcategories, including intelligence warfare, psychological warfare, and strategic information warfare.[19] The United States, by contrast, has created and re-created a number of *official* categories, subcategories and "supercategories" of information warfare (and later information operations). In 1994, the United States had developed the notion of "Command and Control Warfare" (C2W), which was the "military component of information warfare." C2W itself had five subcategories at the unclassified level (electronic warfare, deception, physical destruction, Operations Security and Psychological Operations). Since that time, the U.S. has defined and redefined several different analytical categories. The point is not that the U.S. has better categories of information warfare than China – indeed U.S. categories change often – but that the U.S. has developed a systematic method for examining IW and IO, and for thinking about this emerging aspect of conflict. The Chinese appear not to have done so.

interpretations – the discussions of what IW entails – all tend to expand to include any aspect of conflict that involves either computers or the use (or denial) of information.

[19] Wang Baocun, "A Preliminary Analysis of Information Warfare," *Zhongguo Junshi Kexue* (China Military Science) No. 4, 20 November 1997, pp. 102-111. There may be, however, some emerging consensus as to what information warfare does and does not include: it was recently reported that the PLA's Communications Command Academy is offering courses on information warfare, and basing the course on two IW textbooks. *Keji Ribao*, 27 April 1999, p. 1.

As the absence of an agreed definition and the lack of an analytical framework suggests, the Chinese take an extremely broad view of what constitutes information warfare. This might be considered a "holistic" view of IW. While some Chinese authors limit their analysis to what an American might understand as "information warfare," or perhaps "information operations," most Chinese analysts generally use the term to encompass everything that relates to information and warfare: from at least 1995, Chinese authors have used the phrase "information warfare" to refer to an extremely wide range of aspects of future conflict, including computer viruses, hacking, perception management, new Command and Control Systems, the importance of ISR systems, economic or financial attacks, the exploitation of virtual reality or image projection, and what we would term "long range precision strike." In short, the Chinese understanding of IW seems to be so holistic (or elastic) that it can be broadened to include almost any aspect of conflict involving the use of any data, intelligence or information.[20]

There are several possible explanations for this broad view of information warfare, a few of which are worth considering in more detail. First, it may simply be that the IW debate in China – at least, that taking place in the unclassified literature – is too immature to allow for commonly-held definitions and an agreed analytical framework. It should be noted, in this connection, that there is still considerable debate within the U.S. as to just what does and does

[20] See for example the definition offered by Chang Mengxiong: "Information warfare is warfare of firepower attacks and combat commands to obtain and to counter the obtaining of information, to suppress and countersuppress, and to deceive and counterdeceive, as well as to destroy and counter the destruction of sources of information. It is also warfare to win people's minds and boost morale that employs television, radio broadcasting, and leaflets, focusing on the use and preventing use of information." Chang Mengxiong, "Information-Intensified: A Mark of 21st Century Weapons and Military Units," *Guoji Hangkong* (International Aviation), 5 March 1995, p. 1-5. Many other authors are careful to include "digitized units," by which they mean, apparently, units of troops linked together electronically and employing high-end communications equipment and high-tech weaponry. See for example Zhang Dejiu, "In-Depth Information Warfare Is Philosophical Warfare--(Excerpt of) Major General Xu Yanbin's Academic Report at National Defense University," *Jiefangjun Bao* , 13 August 1996, p. 6, and Wang Xusheng, Su Jinhai, and Zhang Hong, untitled article in *Jisuanji Shijie* (China Computerworld), 11 August 1997, p. 21.

not constitute information warfare (although our feeling is that there is more clarity and uniformity among Western IW analysts). Similarly, it may be that so many aspects of future warfare – C4ISR, precision strike, virtual reality, hacking attacks, and so on – are so far beyond China's current capabilities that they are grouped together, intellectually, simply by virtue of being similarly remote.

An alternative explanation is that there may not yet be elements of the Chinese military bureaucracy charged with the development or prosecution of the various elements of IW: in the absence of a bureaucratic interest, it may be difficult to disaggregate the complex picture of future conflict and to achieve agreement on anything. This possibility is particularly intriguing. The United States was unable to develop a definition and agreed framework of information warfare and information operations until various elements of the DoD and Joint Staff bureaucracies had worked out some sort of a division of responsibilities.[21] Thus, we may find, in the future, that a more developed bureaucratic organization and a more coherent framework develop together.

Finally, it may simply be the case that the Chinese approach to understanding broad problems is substantially different from a Western approach: rather than attempt to divide the problem into components, as we tend to do (and have done with IW), the Chinese may incline toward taking the problem as a whole. It may be well worth further research – perhaps into the nature of the Chinese bureaucracy, or patterns of Chinese intellectual history – to help us understand this aspect of strategic debate in China.

[21] James C. Mulvenon of the RAND Corporation is working on an unclassified paper concerning information warfare and the Chinese bureaucracy. He has already prepared a classified paper that we did not use for this analysis.

Information Warfare as the First Phase of Combat

There is a tendency among Chinese analysts to refer to information warfare as "soft combat," or the damage inflicted through IW/IO as "soft casualties." These "soft" aspects of conflict are contrasted to "hard" combat, generally used to refer to physical destruction and human casualties. Many authors have made this distinction as part of a larger point about the limitations of information warfare: we found no significant evidence of belief that information warfare alone would become an effective method of warfare.[22] (Although over the time period of this analysis we did find a decline in assertions about the limitations of IW or "soft combat" attacks.) Instead, most analysts appear to see the "soft" and "hard" aspects of combat as complementary. The particular role for IW "soft" attacks, in the view of these analysts, is in the initial phases of war. There has been a great deal of discussion about the possibility of each side employing the tools of information warfare to blind, paralyze, or confuse the enemy before launching precision-strike or other sorts of conventional attacks. In many cases, discussions of IW as the initial stage of conflict are linked to assertions about the importance of seizing the initiative, which many

[22] On the limitations of information warfare, see Su Enze, "Logical Concept of Information Warfare," *Jiefangjun Bao* , 11 June 1996, p. 6; Liu Fengcheng and Yu Shuangquan, "Concentrate Forces in New Ways in Modern Warfare," *Jiefangjun Bao* 21 November 1995, p. 6. Although there has been less discussion along these lines in recent years, in 1999 one author did assert that "Internet warfare is a case of easy to defend and hard to attack, with its effects still being hardly satisfactory," due to the fact that internet attacks are constructed similarly, that electronic systems generally recuperate quickly, and that there are simply limits to what internet attacks can accomplish. Shen Weili, "Stressing the Study of Internet Combat," *Jiefangjun Bao* , 27 July 1999. For articles representative of the thinking that "hard" and "soft" attacks should be combined, see Li Yinnian and Li Zongjian, "Network: Dominator of Future Battlefield," *Jiefangjun Bao* , 21 July 1998, p. 6, and Liu Ping, "Some Remarks on Future Psychological Warfare," *Jiefangjun Bao* 18 August 1998, p.6. Liu writes that "The future psychological warfare in the context of high technology is such that while using large quantities of high-technology weapons to cause 'hard destruction,' the belligerent parties also try to cause 'soft destruction' to each other and devastate or weaken the fighting capabilities of the other side on a mental plane, by using as weapons special information media, including language, texts, images, and sound, through modern means and channels of transmission. Many new characteristics have emerged in comparison with the psychological warfare in previous wars." For the best overview of "soft" vs. "hard" combat effectiveness, see Zhou Sijun, "Soft Combat Effectiveness – A New Type of Combat Effectiveness," *Jiefangjun Bao* , 22 January 1999, p. 6.

believe will be particularly vital in the rapidly-fought wars of the future.[23] Interestingly, this line of thinking is particularly prominent among authors with advanced military ranks and those writing lengthy, more analytically developed articles in journals such as *China Military Defense*. This suggests the possibility that the sorts of IW capabilities China eventually works to obtain will be particularly suited to rapid, short-term attacks intended to disrupt rather than permanently incapacitate, which in turn may offer insights into how the U.S. ought to think about orienting its defenses.

Chinese View of IW: Offense

Operational and Tactical level: As has already been discussed, most Chinese analysts tend to view IW as a preliminary stage in conflict, in which both sides make an effort to disrupt or impede the enemy and seize the initiative. In this context, there is also is a tendency to focus much more on the operational level of information warfare than the strategic level. Particularly from 1995-1997 the Chinese, in the unclassified realm, exerted far more effort in understanding how IW might be used against U.S. battlefield forces than in thinking about strategic-level attacks against the U.S. homeland or information infrastructure (they similarly appeared to be more interested in U.S. battlefield, operational-level IW capabilities than in the possibility of American information warfare attacks against Chinese civil targets). Indeed, until relatively recently, the only references to *strategic* information warfare came as passing mention of what U.S. analysts were thinking.

[23] See in particular Huai Guomo (Lieutenant General and COSTIND Vice Minister), "On Meeting the Challenge of the New Military Revolution," *Zhongguo Junshi Kexue* (China Military Science), 20 February 1996, and Huang Xing and Zuo Quandian (both Senior Colonels), "'Holding the Initiative in Our Hands in Conducting Operations, Giving Full Play to Our Own Advantages to Defeat Our Enemy': A Study of the Core Idea of the Operational Doctrine of the People's Liberation Army," *Zhongguo Junshi Kexue* (China Military Science), 20 November 1996, pp. 49-56.

This interest in operational level IO and IW is complemented by a clear bias in favor of using these tools offensively. There is very little discussion of defense: Chinese IW theorists spend the vast majority of their time writing about the offensive systems the U.S. might have (and, by implication, that the Chinese might emulate or eventually face in combat) or how IW might be used to weaken U.S. forces. Even more striking is the degree to which discussion tends to concentrate on the effects that information warfare will have on land warfare. There is remarkably little interest in IW as a component of air or naval warfare, and in those rare instances in which authors do address IW in air or naval warfare, these discussions usually focus on what might be called "jointness." That is, Chinese analysts seem concerned, mostly, with how information warfare might be used to attack the enemy's ability to coordinate its land forces with air and naval support.[24]

When discussing offensive IW – particularly ground-oriented, battlefield IW – most Chinese authors appear to make certain assumptions about the character of future warfare. One of the principal beliefs held by most Chinese IW theorists is that war in the future will consist primarily of a battle of competing military systems, each of which is held together by a network of communications. One of the principal goals of warfare, in this context, is the destruction of the enemy's ability to coordinate and integrate his forces: once the system is broken, physical destruction of the forces is much less difficult.[25] A second widely-held tenet is that future

[24] Interestingly, even in discussions of Kosovo, Chinese analysts express little interest in detailed examinations of how U.S./NATO planes might have been made vulnerable to IW.

[25] Perhaps the best explication of this concept comes from Wang Baocun, who has written that "Confrontation and contests between systems has become a prominent feature of information warfare. Obviously, under these circumstances, only by carrying out a damaging or destructive attack against the critical links making up the enemy's combat system, destroying his battlefield structure, paralyzing his combat system, and fundamentally weakening the enemy's ability to resist, will one be able to effectively alter the relative strength of your forces and the enemy's forces and thereby win victory in war." Wang Baocun, "A Preliminary Analysis of Information Warfare," *Zhongguo Junshi Kexue* (China Military Science), No. 4, 20 November 1997, pp. 102-111. Huang Xing and Zuo Quandian, "Holding the Initiative in Our Hands in Conducting Operations, giving Fully Play to Our Own Advantages to Defeat Our Enemy: A Study of the Core Idea of the Operational Doctrine of the People's Liberation

warfare will be at a much higher tempo than it is today, and that the opening stages will be critical to seizing the initiative. Thus, Chinese analysts tend also to place a premium on attacking the enemy's ability to act quickly or appropriately. (This corresponds, roughly, to the strain of IW thought in the United States that focuses on OODA loops.)

Given these goals, most Chinese IW theorists tend to focus on the methods of IW attack that concentrate on disrupting an enemy's information system or ability to coordinate. By and large, therefore, there is a great deal of discussion of IW weapons and methods with which U.S. analysts are familiar. There is much discussion of jamming and electronic warfare (what one author referred to as "information transmission confrontation"); "hacking" or Computer Network Attacks to disrupt information flows or insert to misinformation to affect decisionmaking; and of inserting viruses to disable enemy communications and coordination.[26] It is particularly interesting to note that the Chinese seem more enamored with viruses and other forms of malicious code than they are with hacking – a direct contrast with the analysis in the United

Army," *Zhongguo Junshi Kexue* (China Military Science), 20 November 1996, pp. 49-56. Somewhat more recently, two analysts wrote that "information warfare aims at wrecking the organizational structure from the very beginning and accelerating the loss of operational functions through structural disintegration. In other words, it first cuts off command and paralyzes the structure, before annihilating the numerical strength and wiping out the function." Wang Jianghuai and Lin Dong, "Viewing Our Army's Quality Building From the Perspective of What Information Warfare Demands," *Jiefangjun Bao* (Liberation Daily) 3 March 1998, p. 6, FBIS-CHI-98-072.

[26] In defining "information transmission warfare," the author suggested that it "should focus upon jamming or counter-jamming of radar or automatic command systems, smooth or timely command information transmission, or timely jamming or disruption of the enemy's command information." Cheng Bingwen, "Step Up Command Confrontation Training," *Jiefangjun Bao* , 27 October 1998, p. 6. A somewhat broader interpretation was offered in 1996, when one analyst argued that electromagnetic warfare should be considered to include not just jamming, but the use of electromagnetic waves to create false targets in enemy targeting systems as well efforts to conceal the sources of their own electronic equipment. See Wu Wenjun, "Modern Air Raid Resistance Tactics," *Jiefangjun Bao* , 9 July 1996, p. 6. At least one author has noted with concern that the United States has developed EMP weapons, writing that "the U.S. National Laboratory has developed a briefcase-size device capable of generating electromagnetic pulses. . . that will burn all electronic devices" located nearby. Geng Haijin, "All Types of 'Computer Warfare Weapons,'" *Jiefangjun Bao* 20 August 1996, p. 6.

States.[27] This may derive, at least in part, from the fact that viruses tend to be far more prevalent in Asia than in the United States, whereas in the U.S., hacking Defense Department and other government sites has become a pastime for some. Whatever the reason, there are frequent references to weapons such as "logic bombs" that could be inserted prior to conflict and activated, remotely, in the early stages of conflict (there is a much-repeated story of U.S. success in undertaking this sort of operation in the Gulf War) or the prospect of a so-called "virus gun" capable of inserting, from a distance, viruses into enemy computer systems.[28] Of course, Chinese analysts do make reference to other sorts of information warfare, including technologies such as virtual reality, particularly as a means of frightening, confusing, or disorienting enemy troops.[29]

[27] See, for example, Chou His, "Exploration and Analysis of Military Computer Security and Virus Protection," *Hsien-Tai Chun-Shi* (CONMILIT), 11 January 1996; there also appears to be interest in counter-virus measures. See FBIS summary of an article by Liu Naiqi and Zuo Zhihong, in *Chengdu Dianzi Daxue Xuebao* (Journal of University of Electronic Science and Technology of China, vol. 26, No. 3, June 1997, pp. 283-288, titled by FBIS as "Computer Virus Countermeasures, Virus Warfare."

[28] The story of virus-infected printers in the Gulf War has been told and re-told several times. See, among other articles, Xu Runjun, Chen Xinzhong, "Computer Virus Weapons," *Guofang* (National Defense), 15 February 1997, No. 2, p. 42-44; Cai Delu and Li Ruifeng, "Electronic Security Technologies, Standards," *Zhongguo Dianzi Bao* (China Electronics News), 21 January 1997, p. 11. On the matter of "virus guns," one pair of authors has written that, "with the assistance of electromagnetic waves," viruses "can be inserted remotely into an opponent's airplanes, tanks, submarines, and other tactical systems, so that when it is activated under certain conditions it will have a destructive effect, destroying computers and processing equipment selectively, particularly automated operational command systems and advanced weapons systems." Xu Runjun, Chen Xinzhong, "Computer Virus Weapons," *Guofang* (National Defense), 15 February 1997, No. 2, p. 42-44. See also Chen Zhaohai, "Computer Warfare Tactics," *Jiefangjun Bao*, 7 July 1998, p. 6, and, for a more farfetched vision of the power of "virus guns," Geng Haijin, "All Types of 'Computer Warfare Weapons,'" *Jiefangjun Bao* 20 August 1996, p. 6.

[29] Perhaps the most colorful passage comes from Wang Baocun, a senior colonel and influential IW theorist, who in 1997 wrote that "In the future, when the U.S. engages in combat with Iran, they plan to display a holographic image of Allah in the air, having this lifelike Allah urge the Iranian soldiers to surrender." Wang further writes: "U.S. Army psyops units conducted experiments in this area during the peace-keeping [mission] in Somalia. Related materials provide the following report on this: On 1 February 1993, at a place 15 kilometers west of Mogadishu in Somalia, a sudden sandstorm came up, and at the same time a 150-200 meter high holographic icon of Jesus Christ appeared amid the murky sands. Seeing this, quite a few of the American peace-keeping soldiers fell to their knees to pray." Wang Baocun, "A Preliminary Analysis of Information Warfare," *Zhongguo Junshi Kexue* (China Military Science) No. 4, 20 November 1997, p. 102-111. A 1997 article discussed recent Chinese advances in virtual reality, but approached the technology mostly as a possible boon to training and combat simulation. Liu

When discussing the operational level of information warfare, Chinese authors tend to talk about both what might be done against the U.S. and, interestingly, what sorts of weapons they have heard that United States has developed or is developing. The Chinese have mentioned explicitly computer viruses, electromagnetic-pulse (EMP) weapons, microwave weapons, and "virus guns." Interestingly, however, these discussions do not have much flavor of fear or concern; rather, the focus appears to be on what may be technologically possible. The Chinese appear to be interested, in short, more in the possibility of developing such weapons than concerned about the ways in which such weapons may be used against them. It is also interesting that, in reporting American IW weapons, the Chinese do not pay much attention to technological plausibility. Reports of "virus guns" are certainly an example. In another instance, an author wrote of American use of "holographic technology" in Somalia, which was purportedly so effective that "witnesses were all filled with mortal fear and knelt down to pray, saying that they would heed 'the messages from Heaven.'"[30]

Strategic Level: As mentioned earlier, there is some evidence, in the more recent unclassified writings, of increasing interest in strategic information warfare–that is, information warfare attacks focusing on long-range attacks against U.S. forces or attacks on the U.S. national infrastructure. Over the past 12-18 months several articles, as well as a lengthy translation of a RAND paper on strategic IW, have appeared in Chinese publications. Before embarking on a content analysis, it should be noted that while these articles are different from earlier writings in that they are devoted more or less exclusively to strategic IW, there is still little evidence of truly

Shihua: "Tour of All-Military Training Simulation Equipment Achievements Exhibition," Hong Kong *HSIEN-TAI CHUN-SHI* (CONMILIT), 11 March 1997, p. 19.

[30] Ibid. See also, Zhang Bibo and Zhang Song, "New Subjects of Study Brought About by Information Warfare – Summary of Army Command Academy Seminar on 'Confrontation of Command on Information Battlefield'" *Jiefangjun Bao* , 20 December 1997.

innovative thinking: most articles seem derivative and based largely on U.S. sources. There is, moreover, no evidence of efforts to think through an entire strategic IW campaign, or even to consider seriously how multiple aspects of strategic IW might be combined to produce dramatic effects. Perhaps most significantly, there is, at the strategic level, little sense that most analysts have a clear grasp of what sorts of goals or objectives information warfare might be used to achieve.[31]

One of the most interesting aspects of Chinese writings on strategic IW is the tendency of many authors to frame the discussion in terms of nuclear weapons, or to make reference to information warfare as a replacement for (or alternative to) nuclear weapons. Several different authors have argued that the effects of information warfare will approach, if not surpass, the effects of nuclear warfare.[32] Others argue that a strategic information warfare capability will emerge as the new strategic deterrent; that an “information warfare umbrella” will replace the “nuclear umbrella” of the past 50 years.[33] Perhaps most interesting, and more revealing, are the passing references –

[31] Among the most developed articles on strategic IW are Yang Minqing, “Facing the Future Information War,” *Jingji Cankao Bao*, 15 October 1999, p. 5 and Wang Xiaodong, “Special Means of Warfare in thc Information Age: Strategic Information Warfare,” *Jainchuan Zhishi* (Internet Version), 30 June 1999.

[32] As early as 1996, one analyst quoted an adviser to a U.S. company as saying that “‘Fighting a war with computers is more effective than fighting a war with nuclear weapons. To destroy the United States, an enemy state will now just try to disrupt the U.S. computer system in a hi-tech fashion and steal $160 billion in one second so that the entire U.S. economy will fall apart.’" Geng Haijun, “All Types of `Computer Warfare Weapons.'" *Jiefangjun Bao* , 20 August 1996, p. 6. More recently, Shen Weiguang, an influential IW theorist, wrote that in future war “The main decisive element to change is from possessing great amounts of material and manpower to possessing great amounts of information and depending on the mastery of information and information warfare capability. It seems that this warfare has become more "civilized" and easier. However, in actual fact the arrival of information warfare and the appearance of information weaponry will cause extremely great damage to mankind. The damage created by information warfare can be described as greater than that caused by nuclear warfare. So far, we have only seen the "civilized" side of information warfare, but not yet deeply recognized the harmfulness of it.” Shen Weiguang, “Checking Information Warfare -- Epoch Mission of Intellectual Military" *Jiefangjun Bao* , 2 February 1999, p. 6.

[33] A number of authors make passing reference to “information deterrence,” but very few elaborate on what the term is intended to mean. The reference to the “information warfare umbrella” is in fact taken from Admiral William Owens, who is quoted as declaring that “What is important is not the size of the aircraft carrier or the Air Force, but the size of our intelligence and our capacity to think and use the information umbrella, which can replace the nuclear umbrella." Lu Xiuru and Yu Zhengxue: "Forecasting the Trend of War in the Era of Intellectual Economy,”

almost casual – to nuclear weapons and nuclear warfare, which appear to indicate a tendency on the part of many IW strategists to think of these two aspects of competition and conflict as similar or somehow related.[34]

Another intriguing aspect of Chinese writing about information warfare at the strategic level is that, so far as we have seen, there has been virtually no mention of the idea of using information warfare as a strategic-level counterforce weapon (i.e. focused on CONUS-based military forces preparing to deploy); discussions of the force-on-force utility of IW are focused entirely on the operational level.[35] Further, there appears to be little interest in the compellence aspects of a strategic information warfare capability, nor is there evidence of a belief that a manifest IW

Jiefangjun Bao , 6 April 1999, p. 6. In 1997, another article cited this same quotation, ascribing it simply to "high-level leaders in the U.S. military." Liang Zhenxing, paper presented at the 15 September 97 Defense Information Modernization and printed in *Zhongguo Dianzi Bao* (China Electronics News), 24 October 1997, p. 8. Symposium organized by the Chinese Electronics Society.

[34] For example, in one 1999 article Shen Weiguang maintained that "Just as the purpose of China's possession of nuclear weapons is twofold, to end the nuclear monopoly and stop nuclear wars, so also is the purpose of China's research on information warfare, to prevent this new war monster from wreaking havoc on mankind and to create an international safety environment favorable to peace and development. Only when we possess the capability to win and make preparations to win can we possibly realize the aim of checking the warfare." Shen Weiguang, "Checking Information Warfare -- Epoch Mission of Intellectual Military" *Jiefangjun Bao* , 2 February 1999, p. 6. Another 1999 article drew comparisons (and distinctions) between nuclear weapons and information warfare, and ultimately concluded that the two had become intimately intertwined; that both must be thought of "under the shadow" of the other. Wu Jianguo and Li Hongbin, "Can Information Weapons Replace Nuclear Weapons?" *Jiefangjun Bao* , 17 November 1999, p. 5. One possible explanation for this, of course, is simply that both nuclear weapons and information warfare tools and techniques could be considered revolutionary military technologies.

[35] In a conversation with us, RAND analyst James Mulvenon suggested that the Chinese might, under some circumstances, be expected to begin a war against the U.S. with an IW attack. See Mulvenon's chapter, "The PLA and Information Warfare," in Mulvenon and Richard H. Yang, eds., *The People's Liberation Army in the Information Age* (RAND Paper CF-145, 1999). There is a story, repeated often in the Chinese IW literature, that the United States inserted viruses into the Iraqi air defense system through previously-infected printers. The case could be made that this represents "strategic information warfare" and that the interest this story has aroused among the Chinese indicates a broader interest in the potential of information warfare to disrupt or disable an enemy's forces and defenses at the strategic level. We have not seen, however, any effort to draw this lesson from the story, or to use the story as a springboard to discussion of the potential implications of strategic IW.

capability would bring with it international prestige or could be used to bully the United States or other nations.[36]

For the most part, then, when the Chinese address the idea of strategic information warfare, there is a tendency to focus on civil targets and to discuss applications of strategic IW rather than the benefits to be derived from simply possessing the capability. In terms of the sorts of attacks Chinese analysts appear most interested in, the majority of attention is devoted to relatively standard sorts of attacks, such as inserting viruses (there has been much attention paid to the Morris Worm) and, more recently, website hacking.[37] In particular, the recent China-Taiwan internet fracas has received a great deal of attention.[38] There is also considerable interest in efforts to exploit the media; in how, during the conflict over Kosovo, the United States successfully manipulated the international media to portray itself as the defender of liberty against the tyrant Milosevic and to U.S. attempts to influence the media within Serbia. This strain of thought is essentially traditional psychological warfare taken to the strategic level and expanded to include digital alteration, the use of the internet, and other innovations of the

[36] There is, however, evident concern that the United States will continue to exploit its dominant military position and behave as a regional and global "hegemon.". Perhaps the most complete argument along these lines came in 1999, when one analyst authored a lengthy article detailing U.S. "hegemonic" aspirations, citing in particular America's efforts to dominate militarily, strategically, and economically, all standing as part of a national strategy for "dominating the whole world." Qin Zong, "Guard Against New Development of U.S. Hegemonism," *Qiushi*, No. 12, 16 June 1999, pp. 12-15. In another article, the author charges that the United States conducted the air war against Yugoslavia largely in order to demonstrate its tremendous military capabilities and "flaunt its wealth and its real military strength before the world, and before third world countries in particular. The author continued to describe the U.S. "China threat theory" as a complex effort to simultaneously publicly belittle China and paint China as an emerging threat. Yang Minqing, "Facing the Future Information War," *Jingji Cankao*, 15 October 1999, p. 5.

[37] Xu Runjun, Chen Xinzhong: "Computer Virus Weapons," Beijing Guofang (National Defense), 15 February 1997, p. 2. On the Morris Worm, see Geng Haijun, "All Types of `Computer Warfare Weapons,'" *Jiefangjun Bao* , 20 August 1996, p. 6, and Chen Zhaohai, "Computer Warfare Tactics," *Jiefangjun Bao* , 7 July 1998, p. 6. For a fairly comprehensive discussion of computer viruses, see Chou Hsi, "Exploration and Analysis of Military Computer Security and Virus Protection," *Hsien-Tai Chun-Shi* (CONMILIT), 11 January 1996.

[38] Both Taiwan and the PRC have exchanged electronic attacks, mostly hacking attacks into web sites, in the wake of Lee Teng-hui's public declaration that Taiwan and the PRC should be considered separate states.

modern information age.[39] Finally, there appears to be a nascent interest in using information warfare techniques to inflict financial or economic damage. This includes attacks on financial institutions as well as a broader concern with the possibility of manipulating national or regional economies.[40]

What we have seen, in short, is a tendency to concentrate on offensive IW focused at the operational level of war intended primarily to weaken or delay U.S. forces. Writings on strategic

[39] For example, one article discusses American plans, in the event of another war against Iraq, to employ "morphology technology" to "fabricate the likeness of a smiling and flawless Saddam, and spread false information through his mouth, so as to strike at the Iraqi military's will and comprehension. At the same time, they will use intercontinental cannon (atmospheric or electromagnetic cannon) to fire non-lethal warheads and create dazzling lights and deafening noise in the sky over Baghdad, to cause confusion and paralysis in Iraqi society." Kong Lingtong, *Liaowang*, No. 45, 8 November 1999, p. 29. This sort of strategic psychological warfare has been the most enduring aspect of Chinese writings about strategic information warfare: since at least 1995, analysts have been discussing the ways in which modern communications and electronics might be used to more effectively wage psychological warfare. Representative of this is a 1995 article by Chang Mengxiong, in which the author notes the importance of IW as an instrument of "psychological warfare, i.e., the use of television, radio broadcasts, and leaflets to win the people's minds and boost morale, waging an information war favorable to one's own side and unfavorable to the opponent." Chang Mengxiong, "Information Intensified – A Mark of 21st-Century Weapons and Military Units," *Guoji Hangkong* (International Aviation), 5 March 1995, No. 3, pp. 1-5. More recently, another analyst has argued that recent revolutions in information technology have made it possible to wage "strategic psychological warfare," coordinating the use of television, digital image-alteration equipment, and other disinformation tools. See Liu Ping, "Some Remarks on Future Psychological Warfare," *Jiefangjun Bao* , 31 August 1998, p. 6. Another article pointed to the potential of information technology and IW to exploit a U.S. vulnerability to psychological warfare, drawing particular attention to the "panic" created by CNN coverage of U.S. casualties suffered in the Gulf War. Zhou Demin, "Dialectic View of Information Advantages and Disadvantages," *Jiefangjun Bao* , 20 May 1998, p. 6.

[40] For example, Wang Baocun has described "economic information warfare" as "infomration warfare whose purpose is to undermine the enemy's economy, including economic information attacks and economic information blockades." Wang pointed out that America's dependence upon electronic financial transfers makes the U.S. a prime target for IW attacks. As for "information blockades," Wang describes them as "cutting off the enemy country's links to external economic information, and its effects are determined by the enemy country's degree of reliance on foreign trade." Wang Baocun, "A Preliminary Analysis of Information Warfare," *Zhongguo Junshi Kexue* (China Military Science), No. 4, 20 November 1997, pp. 102-111. See also "Preparation for 'War of Financial Transactions' Urged," Zhongguo Xinwen She, 1 March 1998. Economic and financial warfare is also a prominent theme in the recently-released Unlimited Warfare. Here, the authors contend that international financiers such as George Soros can engineer regional economic crises, and indicate that Soros and others worked to bring about, or at least capitalize upon, the recent Asian crisis. Qiao Liang and Wang Xiangsui, *Unrestricted Warfare* (Beijing: PLA Literature and Arts Publishing House, February 1999).

information warfare reveal that thinking in this area is still in the very preliminary stages, but that interest is growing and may be expected to continue to grow over the years ahead.

Chinese View of IW: Defense

As previously noted, Chinese IW analysts are clearly much more intrigued by the possibilities of offensive IW than they are concerned about defending against information warfare attacks – a product (most likely) of China's relative lack of dependence upon computers and information systems and a general belief that the nature of information warfare favors the offense. Most often, of course, analysts argue that the best defense is a good offense, focusing primarily on the importance of seizing the initiative and incapacitating the enemy first. Those few discussions of IW defense that do appear tend, moreover, to be rather superficial and to give little sense of technological sophistication. This is not to say, however, that the topic is ignored entirely. There is, for example, some interest in defense at the operational level: because most analysts envision a future conflict in which the preservation of command and control is critical, there has been some attention paid to the problem of maintaining C^2 in the face of enemy IW/IO. There has been as well some discussion and analysis of active defense measures, such as anti-interference and virus-resistance efforts.[41]

More common – and probably more significant – are examinations of possible countermeasures. By far the most often-discussed sorts of measures are those which focus on low-tech responses to anticipated high-tech IO attacks. For example, some analysts suggest that China delay modernization of communications equipment in order to defer or avoid the concomitant vulnerabilities. More interestingly, there is also some discussion of the importance of a decentralized, distributed command system that does not depend upon the sorts of electronic communications that are likely to be targeted by U.S. information operations. Discussions of the Kosovo conflict often include mention of Serb countermeasures: at one workshop, conducted for division and brigade chiefs of staff and organized by the Communications Command Academy, there was considerable attention to the Serbs' success in evading air strikes through maintaining constant mobility or confusing PGMs with fires, smoke, and other low-tech measures (Chinese views of the Kosovo conflict will be explored in greater detail in a following section).[42]

Defense of China's national information infrastructure has suffered from a similar lack of attention. There is some evidence that the Chinese are becoming slightly more interested in the topic, particularly in the wake of Taiwan's emerging interest in IW and IW defense. As with most writings on information warfare, there has been a great deal of interest in what the United States is doing, and some articles include rather detailed discussions of efforts such as the PCCIP and the DSB study of defense against information warfare.[43] Recent articles have called attention to China's dramatically underdeveloped computer security, and call for information security measures including laws, network-protection technology, dynamic surveillance, and

[41] See in particular Wang Pufeng (Major General and research at the Institute of Military Science), "Meeting the Challenge of Information Warfare," *Zhongguo Junshi Kexue* (China Military Science), No. 1, 20 February 1995, pp. 8-18.

[42] Sun Haicheng, Yang Jie, and Zhang Guoyu, "Let Information Warfare Training Rule the Training Sites: Practice and reflections from the First All-Army Collective Training Session for Division and Brigade Chiefs of Staff in Information Warfare Theory," *Jiefangjun Bao* , 13 July 1999, p. 6. On low-tech IW countermeasures more generally, see Senior Colonel Huang Xing (associate research fellow at the Academy of Military Science) and Senior Colonel Zuo Quandian (research fellow of the Academy of Military Science), "'Holding the Initiative in Our Hands in Conducting Operations, Giving Full Play to Our Own Advantages To Defeat Our Enemy' --A Study of the Core Idea of the Operational Doctrine of the People's Liberation Army," *Zhongguo Junshi Kexue* (China Military Science), 20 November 1996, No. 4, pp. 49-56; and Haung Youfu, Zjang Bibo, and zhang Song, "New Subjects of Study Brought About by Information Warfare: Summary of Army Command Academy Seminar on 'Confrontation of Command on Information Battlefield," *Jiefangjun Bao* , 11 November 1997, p. 6.

[43] Whang Zheng and Ke Jianbo, "IW: An Epoch-Making Revolution in Warfare," *Chengdu Keji Daxue Xuebao*, December 1998, pp. 668-672; and Chou His, "Exploration and Analysis of Military Computer Security and Virus Protection," *Hsien-Tai Chun-Shi* (CONMILIT), 11 January 1996.

diagnostic exercises.[44] Other authors have called for creation of "information protection troops" to police the national information infrastructure and launch defensive counterattacks against intruders.[45] There has also been some attention paid to the problem of early warning, a concern that makes particular sense if considered in light of the general belief that war will begin with information-based attacks.[46]

It is somewhat difficult to know what to make of China's apparently minimal interest in defense against information warfare, particularly in light of the widespread assumption that the U.S. will employ considerable, highly-advanced IW measures in the event of war. It may be that discussions of defense take place at the classified level, or that writing of China's vulnerabilities (even potential vulnerabilities) is forbidden. More likely, we think, is the simplest explanation: Chinese IW theorists are inclined to believe that IW will significantly favor the offense, and generally believe that the most effective defense will be to develop countermeasures rather than direct, symmetric defenses. This is a matter that should be given further thought: if the Chinese are unwilling to analyze, realistically, their own vulnerabilities, this may open tremendous opportunities.

How to Proceed

Chinese IW analysts have devoted a great deal of attention to consideration of how their military – and their nation – can be placed in position to compete in information warfare. As might be expected, this line of thought has been heavily influenced by China's conflicting desires to both

[44] See in particular Jia Xiaowei, "Pay Close Attention to Network Warfare Which has Quietly Arrived," *Jiefangjun Bao* , 24 August 1999, p.6; Shen Weili, "Stressing the Study of Internet Combat," *Jiefangjun Bao* , 27 July 1999, p. 6; and Liu Binghua, "Technical Attacks on Network Information Systems, Security Countermeasures," *Zhongguo Guofang Keji Xinxi* (China Defense Science and Technology Information), June 1997, No. 3, pp. 61-63.

[45] Shen Weiguang, "Checking Information Warfare: Epoch Mission of Intellectual Military," *Jiefangjun Bao* , 2 February 1999, p. 6.

emulate and compete with the United States. For this reason – and for the simple reason that the Chinese military is a vast bureaucracy – there is no single "strategic plan" for defense modernization, nor is there consensus on how the PLA should go about preparing for modern warfare. There are, however, several broad areas for improvement or sorts of advances that receive particular attention from IW analysts.

First among such common themes is the importance of theory; of the need for a new doctrine for information warfare. This has been among the most consistently-sounded themes in Chinese IW writings: virtually every prominent IW analyst has called attention to the need for China to develop a new, individual theory of information warfare. This is considered to be particularly important for China, as many analysts argue that it will be theory that will allow China to succeed with only rudimentary equipment and "defeat the superior with the inferior."[47] Further, many analysts appear to proceed from the assumption (sometimes made explicit) that the information warfare revolution will be one in which technology follows doctrine, meaning that much of China's military modernization will depend upon having at least partly-developed theoretical underpinnings. One author drew a distinction between a "Military Technical Revolution" and a "Revolution in Military Affairs" by drawing attention to the critical role of

[46] Zhao Shuanlong, "The Initial Battle Is the Decisive Battle, and Preparations for Military Struggle in the New Period," *Jiefangjun Bao* , 18 August 1998, p. 6.

[47] In a 1996 China Military Science article, two senior colonels (both researchers at the Academy of Military Science) argued that "For operations under high-tech conditions, an important thing is to improve one's weapons and equipment. This is particularly imminent to our Army, which is still at a low level of modernization. However, in order to defeat a strong enemy, a more important thing is to change our operational doctrine, which may be the key and a short cut to our Army's victory in the future." Huang Xing and Zuo Quandian, "Holding the Initiative in Our Hands in Conducting Operations, Giving Full Play to Our Own Advantages To Defeat Our Enemy--A Study of the Core Idea of the Operational Doctrine of the People's Liberation Army," *Zhongguo Junshi Kexue* (China Military Science), 20 November 1996, No. 4, pp. 49-56. At about the same time, another senior military officer, Lieutenant General Huai Guomo, vice minister of COSTIND, wrote that "We need to intensify our study of the art of war. We need to recognize that as there will still be a gap in the future between our military equipment and that of the developed nations, creating new combat and training tactics to supplement our technological gap would seen to be particularly necessary and pressing." Huai Guomo, "On Meeting the Challenge of the New Military Revolution," *Zhongguo Junshi Kexue* (China Military Science), 20 February 1996.

theory in an RMA (and went on to argue that we are currently in the midst of an RMA, not an MTR).[48] Although these articles are generally positive – emphasizing the vast advantages conferred by theory – authors do sometimes imply that current thinking is inadequate, and at least one author has explicitly criticized prevailing Chinese doctrine.[49] This emphasis on conceptual and doctrinal development brings to the fore concerns about excessive reliance on (or emulation of) the United States. Repeatedly, Chinese IW analysts warn of the dangers of accepting "inherited" concepts and urge the development of IW theories specifically suited to China's strategic situation.[50]

Without doubt the most pronounced theme – which fits well with the focus on theory – is attention to the need to improve training and education. Countless authors have called for training of a particular group, such as commanders, or the creation of a corps of highly-skilled troops for high-tech or information warfare. This emphasis on the creation of elite troops marks a substantial break from traditional notions of "People's War" and appears to be gaining

[48] Frequent "Military Forum" contributor Su Enze has written that "a 'military technological revolution' has happened while a 'military revolution' is happening or is soon to happen. Guided and represented by information technology, a batch of modern hi-tech weapons have been developed and applied to the battlefield. This shows that a 'military technological revolution' has already happened. Guided and represented by 'information warfare,' a 'military revolution' is also taking place in military ideology, military theory, military establishment, combat pattern, and other military fields on a global scale." Su Enze, "Logical Concept of Information Warfare," *Jiefangjun Bao* 11 June 1996, p. 6.

[49] Su Enze, in a rather lengthy "Military Forum article," urged Chinese analysts to become "more emancipated," arguing that current theory is "too low-tech,", "too showy," lacking in experimental data, and too hidebound. Su Enze, "A Personal Look at the Innovations in China's Military Theory," *Jiefangjun Bao* 15 December 1998, p. 6.

[50] One author declared that "Countries which are lagging behind in the informatization process appear to be lagging behind in "hard" technology, but they are actually lagging behind in "soft" thinking. A new mode of thinking needs new concepts in the first place, and new concepts can only come from new practice and the absorption and assimilation of new things," and went on to warn that "A total takeover of foreign technology and theoretical concepts will lead to abnormal thinking." Zhang Jiali, "Is It True 'There Is A Shortcut to Informatization'?" *Jiefangjun Bao* 14 July 1998, p. 6. Another writer argued that "On the study of operational theories, it is necessary to stop echoing the views of others, and truly get a clear understanding of the characteristics and laws of the wars which will be confronting our country, as well as of the modes of confrontational actions and possible hi-tech means to be taken, in order to provide correct guidance to training." Xiao Yunhong, "Advance Training Reform with Science and Technology Progress," *Jiefangjun Bao* 11 August 1998, p. 6.

adherents as the most appropriate way of advancing China's military capability. Others focus instead on the need to train all troops to achieve some base level of familiarity with technology and the concepts of information warfare. Interestingly, many of these articles appear in *Jiefangun Bao*, meaning that in some sense the articles are in themselves an effort to train.[51] Other articles reveal a somewhat broader perspective, focusing on the need to educate the general populace: without educated society comfortable with new technologies, these authors contend, China will lack a suitable foundation for development of a high-tech military (although as mentioned very few authors indicated a belief that the general populace should be trained to wage information warfare).[52] It should be noted that while calls for reforms to education and

[51] The following passage is representative: "in order to hone this sword [i.e., the PLA] to incomparable sharpness, the best way of doing so is to train and develop ahead of time a large quantity of talent specialized in high technology, but not fall behind the enemy. Once the nation has these talented people, it can both speed up development of high-tech weapons while also bringing out the potential efficiency of a few purchased weapons. . . . It is sufficient to point out that human resources' qualifications cannot be imported, and modernization cannot be bought. If we say that in traditional war "an uneducated army is a stupid army," then in modern war, an army that does not know science and technology is an impotent army. Dexterous weapons need dexterous soldiers, and with warfare so highly technical, the traditional method of comparing military strength purely on a basis of military manpower and weapons is obsolete, for intellectual training is becoming more important than physical training." Major General Huang Dongjia, "Changes in the 'Good or Bad View' and Chinese Military Modernization," *Hsien-Tai Chun-Shih* (Conmilit), 11 January 1997, No. 240, pp. 23-24. For recent articles along these lines see for example Liu Linfu, "Advance Training and Reservation of Military Personnel," *Jiefangjun Bao* 9 May 1999, p. 2; Shan Aidong, "Network Training: Important Way for Training Troops with Scientific and Technological Means," *Jiefangjun Bao* 19 October 1999, p. 6; and in particular Sun Haicheng, Yang Jie, and Zhang Guoyu, "Let Information Warfare Training Rule the Training Sites: Practice and Reflections from the First All-Army Collective Training Session for Division and Brigade Chiefs in Information Warfare Theory," *Jiefangjun Bao* 13 July 1999, p. 6. Older articles include Wang Pufeng, "Meeting the Challenge of Information Warfare," Johngguo Junshi Kexue (China Military Science), 20 February 1995, No. 1, pp. 8-18 and Liu Senshan, "Servicemen Should Have `Electronic Accomplishments,'" *Jiefangjun Bao* 16 April 1996, p. 6. Lei Zhuomin focused particularly on commanders (arguing that they would be the centerpiece of any advanced military, while another article drew attention to the need to educate the entire military: "We need to cultivate talent suited to information warfare. . . . As to cadre training, all cadres at all levels need to endeavor to learn information technology and information warfare knowledge. In training reform, we need to add substance on information confrontation all the way from basic training to battle tactics drills." Niu Li, Tan Haitao, and Liu Jainguo, "Information Warfare is Coming at Us," *Jiefangjun Bao* 28 March 1995, p. 6.

[52] Representative of this is a comment made by a graduate student during a symposium on the RMA: "Back in the Cold War era, some strategists already touted the concept of combining civilians with military. In the age of the knowledge economy, integration alone is not enough. The trend to integrate civilians with the military is already here. . . . At a time when China's knowledge economy remains underdeveloped, the only way to effect the strategic

training are extremely frequent, it is only rarely that an author proposes, with any specificity, what actually ought to be done.[53] We did see, beginning in last twelve months or so, a few references to steps that have already been taken, mostly the establishment of schools or courses to enhance technical education.[54]

One of the more unexpected – and potentially one of the most significant – themes we uncovered was the discussion about changing military organizations. We found that this discussion concentrated on two different levels of the defense establishment: the military command and, more broadly, the national defense bureaucracy at large. With respect to changing the structure of military command, we found countless proponents of a move toward decentralized command;

shift toward military-civilian integration, to enable military and civilians to help each, and to make China prosperous is to fully utilize local knowledge resources and accelerate the transition toward a knowledge-based military." Another symposium participant later noted that "The key to making the military intelligent is to educate the people. In the era of the knowledge economy, the dividing line between scholar and soldier is getting blurred. The future war is more a confrontation between scholars than a confrontation between soldiers." Zhang Guoyu, "Symposium on Challenge of Knowledge Revolution for the Military," *Jiefangjun Bao* , 5 January 1999, p. 6.

[53] At a 1999 symposium of military officers, one participant did offer a more specific catalogue than most, arguing that "we should also note that irrationalities in the training content, system, and structure have kept information warfare training from truly becoming the mainstream of our military training. At present, information warfare training is in a "do-as-you-please" situation in which the content is not systematic, the operations lack order, there are no assessment standards, and management lacks regulations. To make information warfare training into a main theme in our scientific and technical military training, we cannot just make it an add-on to the original training framework, but should have information warfare training become a principal part of the content of military training in our army, thereby forming a new generation of military training contents and systems in which information warfare training is a primary focus. To do this, we must formulate as quickly as possible a new generation of training rules, centered around information warfare training and including training programs, training courses, assessment standards, and organizational management, etc., using regulations to standardize the overall development and orderly operation of information warfare training." Sun Haicheng, Yang Jie, and Zhang Guoyu, "Let Information Warfare Training Rule the Training Sites: Practice and Reflections from the First All-Army Collective Training Session for Division and Brigade Chiefs of Staff in Information Warfare Theory," *Jiefangjun Bao* 13 July 1999, p. 6.

[54] One recent article in Keji Ribao noted the creation of an IW course as the PLA's Communication Command Academy, which apparently includes an IW curriculum at the Ph.D. level. "PLA Trains Information Warfare Specialists," Keji Ribao, 27 April 1999, p. 1. See also an article by Ma Xiaochun, from the Beijing *Xinhua* Domestic Service (New China News Agency), "PLA Sets up Four New Academies," 02 July 1999, and Si Liang, "Chinese Armed Forces are Increasing Their Capacity for Fighting Electronic Warfare," *Hong Kong Zhongguo Tongxun She*, 9 August 1999.

away from what analysts described as a "pagoda" type of command structure and toward a more distributed structure that accorded much more freedom of action to unit-level commanders.[55] More significant, and more relevant to our study, is the discussion of change at higher levels of the defense establishment. We found, particularly within the more serious periodicals such as *China Military Science*, a number of articles calling for significant bureaucratic shifts. Authors – often senior officers – have called for transforming the logistics system or the procurement system, and others have urged that the military services reorganize along operational lines.[56]

[55] The term was employed by Shen Weiguang in two articles: "Focus of Contemporary World Military Revolution--Introduction To Research in Information Warfare," *Jiefangjun Bao* , 7 November 1995, p. 6, and "Checking Information Warfare -- Epoch Mission of Intellectual Military," *Jiefangjun Bao* 2 February 1999, p. 6. A similar line of thought is evident in a 1998 article, in which the author argues that "As far as the Army building thinking is concerned, information warfare is motivating Army building to switch from the track of functional expansion to the track of structural optimization. The integration of the uses of various armed services through the lateral interlinking of information has become a natural tendency. Networked command will enable joint operations to continuously infiltrate into the tactical level. As the command system is integrated, the operational formation is further coordinated. The light digitized units characterized by modular reorganization and coordination of three services will pose a challenge to the existence of heavy mechanized units." Wang Jianghuai and Lin Dong, "Viewing Our Army's Quality Building From the Perspective of What Information Warfare Demands," *Jiefangjun Bao* , 3 March 1998, p. 6.

[56] The call for reform to the logistics system comes in Lt. Gen. Chen Bingde, "Intensify Study of Military Theory to Ensure Quality Army Building: Learning from Thought and Practice of the Core of the Three Generations of Party Leadership in Studying Military Theory," *Zhongguo Junshi Kexue* (China Military Science) 20 August 1997, No. 3, pp. 49-56. Another article is worth quoting at some length: the author first suggests phasing out obsolete systems to reduce the defense burden, and then argues that "To meet the needs of the military revolution, we will need to gradually reform our purchasing system that was formed in the industrial age. . . . We need to make as much use as possible of civilian technology and equipment, focusing on cultivating the capability when necessary to convert our civilian industrial capacity to a wartime army of civilians. In addition, it will only be when our defense S&T industry takes new management steps such as all-out quality control, timely production, and parallel projects that it will be better able to meet the needs of the military revolution." COSTIND vice-minister and Lt. Gen Huai Guomo, "On Meeting the Challenge of the New Military Revolution," *Zhongguo Junshi Kexue* (China Military Science) 20 February 1996. See also senior colonel Huang Xing and senior colonel Zuo Quandian, "'Holding the Initiative in Our Hands in Conducting Operations, Giving Full Play to Our Own Advantages to Defeat Our Enemy': A Study of the Core Idea of the Operational Doctrine of the People's Liberation Army," *Zhongguo Junshi Kexue* (China Military Science), 20 November 1996, pp. 49-56. Interestingly, U.S. defense analyst Bates Gill has argued that "the greatest obstacles between China and the emergent RMA does not rest in the development of technology so much as in the restructuring of concepts and organizations." Bates Gill, "China and the Revolution in Military Affairs: Assessing Economic and Socio-Cultural Factors," in Gill and Henley, "China and the Revolution in Military Affairs" (Carlisle: U.S. Army War College, 1996), p. 27.

These sorts of suggestions represent some of the most serious thought we have seen given to what China must really do in order to pursue an information warfare capability.

There has been, as well, a great deal of concern over – or at least discussion of – how China ought to go about modernizing its physical equipment and materiel, particularly high-end technical and communications equipment. There is a commonly-voiced belief that, important as training and theory might be, future military might will also depend critically upon advanced equipment, and that China needs to begin, now, to prepare for the future.[57] This debate has included, interestingly, some attention to the increasingly prominent role of "dual use" technologies.[58] As would be expected, there has been considerable attention paid to the tension between the desire to acquire Western technologies and the acknowledged need for China to develop a capacity for self-sufficiency and innovation.[59] There is in particular concern that the West is not only keeping China from achieving technological independence, but also may be supplying China with technology that contains backdoors or latent viruses.[60]

[57] Representative of this line of argument is a 1997 article from *Jiefangjun Bao* which argues that: "To win the information war, we must develop appropriate technical facilities and establish a supporting information war system. Otherwise, if we do not have a minimum stand for entering the information war, our military will become a military under attack." Huang Dongjia (major general and group army deputy commander), "Changes in the 'Good or Bad View' and Chinese Military Modernization," Hong Kong *Hsien-Tai Chun-Shih* (Conmilit), 11 January 1997, No. 240, pp. 23-24. See also Zhang Jiali, "Is It True 'There Is A Shortcut to Informatization'?" *Jiefangjun Bao* 14 July 1998, p. 6.

[58] Chi Haotian, then the defense minister of the PRC, wrote a lengthy article in which he addressed this issue. Chia Haotian, "Taking the Road of National Defense Modernization Which Conforms to China's National Conditions and Reflects the Characteristics of the Times: My Understanding Acquired from the Study of Comrade Jiagn Zemin's Expositions on the Relationship between the Building of National Defense and Economic Development," *Qiushi* (Seeking Truth), 16 April 1996, No. 8, pp. 8-14.

[59] David Roessner has pointed to the historical roots of China's concern with technological dependence, arguing that the Sino-Soviet rift of 1960 deeply marked China and that afterword "the principle of 'self-sufficiency' became a guiding axiom for China." David Roessner and Michael Salamone, "National Technological Competitiveness and the Revolution in Military Affairs" (Joint Management Services Report JMSTR 99.6.1, June 1999), Appendix II, "Military Technology Adaptation and Development in China."

[60] For example, as noted earlier, many Chinese analysts cite a story concerning the Gulf War: Iraq, the story goes, purchased a number of computer printers from the U.S., only to find, once the war began, that these computers held latent viruses that were unleashed, crippling the Iraqi air defense system. One article in particular expressly warns

There are two related undercurrents running through all of these discussions. The first is the ever-present tension between emulation and competition, which has already been examined. The second is the debate over how aggressively China ought to go about modernizing for the future.[61] One analyst described three alternatives. China might proceed in *stages,* preparing for the future slowly, pursuing a follower strategy that would create substantial savings and give them time to learn. Alternatively, China might follow what he called a *"transcendental"* course, skipping the middle stage of development and try to jump to immediate parity with the U.S. (or perhaps even superiority). Finally, the Chinese might adopt a "*comprehensive*" option -- trying to pursue two paths simultaneously, developing traditional mechanized forces for the near term and invest in high-tech forces over the long term.[62] By and large, however, few authors offer a notional plan for modernization or even go so far as to propose priorities: the defense modernization debate, at the unclassified level, takes place in the broadest of terms.[63]

against excessive dependence upon U.S. technology, noting that both Microsoft and Pentium have installed "backdoors" in their exports. The author warned that "Hackers from all countries can enter China's networks like walking on level grounds! . . . if we follow other people and imitate their every move, we will forever be 'doing that we can to catch up' but will not be able to 'catch up.'" He further declared that "Casting aside the 'blind alley' that has been designed for us by our opponents and that is filled with traps and beset by dangers . . . [is the base] for building and developing the information and network technology!" Xu Xiaofang and Dan Aidong, "Serious Challenge to Information Network Security," *Jiefangjun Bao* 20 July 1999, p. 6.

[61] The ongoing defense modernization debate has received considerable analytical attention here in the U.S., and there is little sense in recapitulating those analyses here: probably the best work on this is Mark Stokes, "China's Strategic Modernization: Implications for the United States" (Carlisle, PA: U.S. Army War College, 1999). See also Bates Gill and Lonnie Henley, "China and the Revolution in Military Affairs" (Carlisle: U.S. Army War College, 1996); Zalmay Khalilzad et al, "The United States and a Rising China: Strategic and Military Implications" (RAND Memorandum MR-1082-AF, 1999); and David Roessner and Michael Salamone, "National Technological Competitiveness and the Revolution in Military Affairs" (Joint Management Services Report JMSTR 99.6.1, June 1999), especially Appendix II, "Military Technology Adaptation and Development in China."

[62] These three alternatives were examined by Wang Baocun, who argued that the wisest course was the "comprehensive" development path that would leave China prepared for anything. Wang Baocun, "Military Transformation in an Information Era," *Jiefangjun Bao* 6 May 1998, p. 6.

[63] Perhaps the most developed plan we found came from a *Jiefangjun Bao* article, in which the author argued that China "should at least have started by the end of the 20th century, and basically finished by the middle of the 21st century, to acquire the capability to fully compete with and win an information war with the great powers." The same author gave some sense of top priorities, focusing on the need for an advanced C4I system as a critical first

The overall impression left by these discussions is that of a military organization that has recognized the need to modernize but is still at the very earliest stages of thinking about how this ought to be done. There has been an effort – apparently successful – to identify those aspects of the military that must change, yet there have been few analysts who have offered visions of what a modernized military ought to look like. There is as well very little sense of time: few authors are explicit about when changes ought to be made, which ought to be made first, or what the military ought to look like at some specified point in the future. (This is a characteristic of nearly all of the Chinese writings on IW, but it seems particularly pertinent to the discussions surrounding defense modernization.) There is little sense, in short, of some sort of generally-held strategic vision of how China ought to go about modernizing for future conflict.

Chinese Observations on the Gulf War and Kosovo

As might be expected, Chinese military analysts have paid particularly close attention to America's recent military conflicts. The Gulf War is mentioned frequently, mostly as a milestone in the revolution in military affairs; as a conflict that blended both traditional and future warfare and as the beginning, rather than the end, of the RMA.[64] A few authors have also

step in developing a high-tech military. Zou Fengxing, "Suggestions for Equipping PLA Digitized Military Units," Hong Kong *Hsien-Tai Chun-Shih*, 11 February 1999, pp. 27-28. Some articles do offer a more thorough analysis of defense modernization, but rarely explicitly address military applications such as information warfare. See for example the State Science and Technology Division's National Medium- and Long-Term Science and Technology Development Program, 1990-2000-2020, 1992 (published in English and available through FBIS) and an article by Zhu Lilan, Minister of Science and Technology, "Intensify Technological Innovation, Promote Industrialization, Vitalize Country with Science, Education," *Qiushi*, 1 September 1999, pp. 3-6.

[64] Representative of this is a passage from a 1998 *Jiefangjun Bao* article: "As a military struggle intended to seize information control, the Gulf War ushered in a new war form by turning a local electronic confrontation into a C3I system confrontation in which space-based satellites expanded a battlefield from ground to space and a C3I command and control system ensured an integrated operation involving different arms." Cheng Jian, "Take Information Warfare as Starting Point of Military Struggle Preparations," *Jiefangjun Bao* 2 June 1998, p. 6. Another analyst has written that although "the Gulf War was not an information war in the truest sense of the term, nevertheless in the final analysis it demonstrated an entirely new form of warfare with the leading weapons being information weapons. It also marked the close of the era of warfare in which tanks were the primary weapons on

pointed to the Iraqis as a cautionary example of a U.S. opponent that failed to prepare itself for "informationized" combat. For example, several analysts have told the story of how the U.S implanted viruses in computer printers, sold the printers to the Iraqis, and then in the course of war activated the viruses, disabling the Iraqi air defense system. This story is told not just to demonstrate the potential of IW, but to warn of the dangers of relying upon foreign-supplied technology.[65] There is also some feeling, on the part of some Chinese analysts, that the Iraqi military represents a case study in the inability to develop original concepts and adapt to the realities of future war.[66] Though the overwhelming opinion of Chinese IW analysts is that the Iraqis were a vastly inferior force and were duly routed, at least one analyst has drawn attention to the U.S. weaknesses and vulnerabilities that were revealed over the course of the war against Iraq.[67]

war." Yang Shuqi and Guo Ruobing, "Information Warfare: Hot Topic in Modern Military Circles," *Zhongguo Guofang Keji Xinxi* (China Defense Science & Technology Information), Sep-Dec 1996, No. 5/6, pp. 90-93.

[65] "In the process of building the information network, if we blindly depend on imports of software, hardware, and even encryption technology, and build our information network security on other people's technology, then we are taking "the line anticipated by our opponents." Before the outbreak of the Gulf War, the US Secret Service secretly replaced the wafers in a batch of new printers for air-defense systems that Iraq purchased from France with those that contained computer viruses. When the Gulf War broke out, the US military used wireless remote control devices to activate the viruses hidden in the computers, and paralyzed the Iraqi air-defense system. In an information network era that is filled with competition and conflicts of interest, if we follow other people and imitate their every move, we will forever be 'doing what we can to catch up,' but will not be able to 'catch up.'" Xu Xiaofang and Dan Aidong, "Serious Challenge to Information Network Security," *Jiefangjun Bao* 20 July 1999, p. 6.

[66] "During the Gulf War, Iraq 'took the short cut' by spending huge amounts of money on the purchase of informatized weapons, but they could not buy an informatized mode of thinking. They could only use their industrial mode of thinking to direct troops equipped with weapons which made use of information technology. A total takeover of foreign technology and theoretical concepts will lead to abnormal thinking." Zhang Jiali, "Is It True 'There Is A Shortcut to Informatization'?" *Jiefangjun Bao* 14 July 1998, p. 6. Another author argued that "In the Gulf War, Iraq's advanced weapons, purchased at a high price, became a waste pile because its officers and men were unqualified to operate them. It is sufficient to point out that human resources qualifications cannot be imported, and modernization cannot be bought. Major General Huang Dongjia, "Changes in the 'Good or Bad View" and Chinese Military Modernization," *Hsien-Tai Chun-Shih* (Conmilit) 11 January 1997, No. 240, pp. 23-24.

[67] Two senior colonels wrote that "our enemy's high-tech weapons and equipment are not flawless, but have some weaknesses and shortcomings. Technological development is boundless, which implies, in a sense, that al weapons and equipment, no matter how advanced they may be, have their weaknesses. For instance, the F-117 stealth airplane, which is known as the most sophisticated weapon system of our day, was detected by antiaircraft radar of the Saudi Army many times during the Gulf War; the Slam radiation-resistant missile and the Tomahawk cruise

The Chinese found Kosovo particularly interesting for several reasons. First, there is apparently a growing belief among Chinese defense analysts that U.S./NATO involvement in the crisis and intervention in the domestic affairs of another country exemplifies the U.S. global strategy of "hegemony" and unipolar dominance.[68] (This perspective on the war likely contributed to the shift, noted earlier, toward greater inclination to perceive the U.S. as a threat rather than a model to be emulated.) It is also a commonly-held view that Kosovo represents another significant step toward a true revolution in military affairs, and although few authors argue that the conflict represents the culmination of the RMA most seem to believe that future warfare will look more like Kosovo than the Gulf War. Most of all, there is widespread interest in the Kosovo conflict because the FRY forces fared so much better than anticipated. There is, in this respect, a tendency – often stated explicitly – to regard FRY forces as something of a model to be followed, or at the very least a test-case to be studied intently. While there is some mention of the FRY's use of hacker attacks against U.S. and NATO-related websites, Chinese analysts have drawn particular attention to the Serbs' ability to develop low-tech countermeasures to

missile are required to spend a long time for prelaunch data input and at least 3-4 hours for launch preparations; the AH-64 Apache armed helicopter, claimed to be an all-weather plane, has never had its sortie rate exceeding 80 percent under highly dusty circumstances." Huang Xing and Zuo Quandian, "'Holding the Initiative in Our Hands in Conducting Operations, Giving Full Play to Our Own Advantages to Defeat Our Enemy': A Study of the Core Idea of the Operational Doctrine of the People's Liberation Army," *Zhongguo Junshi Kexue* (China Military Science) 20 November 1996, No. 4, pp. 49-56. To demonstrate the difficulty of changing the military, one analyst argued that "Even in the United States, a qualitative change has yet to take place in the establishment composition of its military system. . . . During the Gulf War, the command system of U.S. troops as a whole was still a tree-type structure rather than a network structure required by information warfare." Cheng Yawn, "Keep Abreast of the Development Pattern of the New Military Revolution," *Jiefangjun Bao* , 7 July 1998, p. 6.

[68] This is a theme common to Chinese articles on future warfare or geopolitics. Representative articles include Cheng Guangzhong, "Kosovo War and the U.S. 'Python' Strategy," *Ta Kung Pao* 2 June 1999, p. B8; Yao Youzhi, "U.S. Strategic Orientation in the 21st Century as Viewed from the Kosovo War," *Zhongguo Junshi Kexue* (China Military Science) 20 May 1999, pp. 11-14; and Liu Mingde, Ma Gang, et al, "FRY Crisis Shows Need to Strengthen PLA," *Jiefangjun Bao* 13 April 1999 (this article is the transcript of a discussion held by National Defense University staff).

U.S./NATO forces.[69] Analysts have praised the Serbs' success concealing their positions, timing the NATO airstrikes, and diverting Western precision-strike munitions.[70] Chinese analysts seem to have been particularly impressed with the FRY's command-and-control system which, many analysts indicate, was organized specifically to reduce vulnerability to U.S./NATO information operations.[71]

While most analysts focused on the relative success of the FRY, there has also been some attention paid to the ways in which the U.S./NATO forces were able to employ IW against the Serbs. At a somewhat general level, many articles have discussed U.S./NATO success with a "nodal" attack intended not to destroy but rather to decapitate and paralyze FRY forces.[72] More

[69] On hacking: "Yugoslavian computer experts acted in unison with hackers in Russia an other countries who were sympathetic with Yugoslavia and launched a concerted attack through the internet on the computer systems in NATO countries, which made the White House's Web sites and the computer system on the aircraft carrier 'Nimitz' difficult to function for a short while. Although the network struggle between the NATO and Yugoslavia could not be called a 'network war' in its true sense, but it still can provide a warning and many lessons for us." Jia Xiaowei, "Pay Close Attention to Network Warfare Which has Quietly Arrived," *Jiefangjun Bao* 24 August 1999, p. 6. See also Wang Baocun, "Information Warfare in Kosovo Conflict," *Jiefangjun Bao* 25 May 1999, p. 6.

[70] "We should emulate the useful experience gained by the FRY in many respects. Yugoslav commanders mobilized their forces according to the time lapses between orbiting reconnaissance satellites overhead. Through analyzing the guidance systems of unexploded missiles, Yugoslav experts found that heat-sensitive sensors, instead of computers they had previously thought, were used for the last flight stage of these guided missiles. They thus set fires to the roofs of garage buildings close to the large infrastructure to direct the cruise missiles into the fires. They also painted the steel parts of bridges and railways with colorful paints to disorient guided missiles' heat-sensitive sensors." Cheng Bingwen, "Countermeasures and Thoughts for Fighting 'No Contact Warfare': on the Need to Refocus Our Preparations for Military Struggle," *Jiefangjun Bao* 4 October 1999, p. 3. See also Sun Haicheng, Yang Jie, and Zhang Guoyu, "Let Information Warfare Training Rule the Training Sites: Practice and Reflections from the First All-Army Collective Training Session for Division and Brigade Chiefs of Staff in Information Warfare Theory," *Jiefangjun Bao* 13 July 1999, p. 6.

[71] One commentator argued that "At present, the organization and command of China's military mainly uses centralized command. Centralized command is highly dependent on the automated command system. When this system is incapacitated or destroyed, it is very difficult for the troops to organize effective action. When the command control system of the FRY military met with powerful electronic interference and artillery fire, the air-defense troops were still able to carry on the air-defense war effectively. Moreover, they shot down numerous NATO aircraft. Their experience is worthy of our study." Liu Mingde, Ma Gang, et al, "FRY Crisis Shows Need to Strengthen PLA," *Jiefangjun Bao* 13 April 1999.

[72] Wang Baocun has discussed U.S./NATO successes, including C4ISR, "beheading" the Serbs' command system, electronic warfare, psychological warfare, and the imposition of an "information blockade" against the Yugoslav

directly related to the utility of information warfare, several analysts have drawn particular attention to the importance of the pre-war contest over shaping world opinion and the inter-war efforts to use the media to turn the populace against Milosevic.[73] Finally, as might be expected, analysts have noted that while FRY forces performed admirably given their limitations, the conflict in Kosovo has underscored the vast advantages of military-technological superiority.[74]

In sum, Chinese analysts are decidedly interested in America's most recent conflicts, partly in terms of bolstering their depiction of the United States as an interventionist "hegemonic" power and partly in an attempt to understand why America's opponents have fared as they have. There is little sense of awe or alarm in these writings: particularly with respect to articles on Kosovo, most authors emphasize Serb successes and tend to depict the U.S. not as all-powerful but rather as simply an unprincipled bully. With respect to information warfare, what is perhaps most notable is that IW is not considered in isolation: Chinese analysts, virtually without exception, address all aspects of IW (including perception management, electronic jamming, and psychological operations) as fundamentally intertwined with the rest of warfare (i.e., nodal air strikes, etc.). It may well be worthwhile to continue to track Chinese analysis of the Kosovo conflict as more articles are written and translated.

military and public populace. Wang Baocun, "Information Warfare in the Kosovo Conflict," *Jiefangjun Bao* 25 May 1999, p. 6. For an analysis of the U.S./NATO "nodal" strategy, see Su Size, "Kosovo War and New Military Theory," *Jiefangjun Bao* 1 June 1999, p. 6.

[73] "Before the war, NATO, led by the U.S., used the mainstream media in the Western nations to greatly distort the real nature of the impending war, seeking to exert a widespread psychological effect on the standpoints and attitudes prevailing in international society. . . . In the early stages of the war, U.S.-led NATO waged war simultaneously on the two main battlefields – the military battlefield and the battlefield of the heart." Yang Minqing, "Facing the Future Information Warfare," *Jingji Cankao Bao* 15 October 1999, p. 5.

[74] One commentator noted that "we should concede that the side with the superior technology will have the larger initiative. . . . This tells us that we must resolutely follow the path of strengthening the army through technology, increase the sense of urgency to modernize national defense, and forcefully develop a unique high-tech weapons system. This will be the basis of our ability to achieve the initiative in a future war." Liu Mingde, Ma Gang, et al, "FRY Crisis Shows Need to Strengthen PLA," *Jiefangjun Bao* 13 April 1999 (this article is the transcript of a discussion held by National Defense University staff).

V. Conclusions

Overall, we found a number of interesting themes in Chinese writings on Information Warfare and Information Operations:

- There appears to be a *deliberate effort to introduce young officers*, non-commissioned officers and PLA soldiers (at least, literate soldiers) to the notions of high technology warfare – especially information warfare and information operations. Moreover, there is explicit recognition of the importance of training – and perhaps the development of elite military forces – as a critical component of preparation for future conflict.

- Throughout the period we examined, the Chinese were inclined to view the United States as both *a model to emulate and as a competitor to frustrate*. This is a difficult position for the Chinese to maintain, and writings on IW betray, at several points, evidence of a struggle to come to some resolution on the matter. It should be noted that there was, in 1999, a shift in emphasis, toward perceiving the U.S. as a competitor (with more interest in countering U.S. capabilities rather than emulating U.S. technologies). Clearly, much of this arose from the conflict over Kosovo: whether this marks the beginning of a new trend or is simply an aberration is unclear at this point – and is well deserving of further attention. In either case, however, it seems clear that for the Chinese, at least with respect to IW, the U.S. is the military to watch: there is markedly little interest in what other powers are doing, a situation that may create real opportunities for the U.S. to influence the directions of Chinese thought and behavior.

- There appears to be *no agreed analytical framework* on IO and IW in China. Absent a common definition and analytical approach, different analysts view information warfare and information operations very differently from one another, but lack the framework and terminology necessary to conduct clear, direct debate. It is unclear whether this is a product of our focus on unclassified writings, the nature of Chinese intellectual traditions, or the immaturity of Chinese thinking on IW.

- Chinese analysts focus on using IW and IO at *the operational and tactical levels of warfare*. Until recently there was very little open discussion of "strategic information warfare" directed against the national infrastructure. Moreover, most of the analysis is concerned with how IO and IW can be used by and for ground forces, rather than air, space or naval forces.

- In most of the serious in-depth analyses we examined, there was a widespread belief that IO and IW would be the *first phase* of armed conflict. IW and IO were seen as mechanisms to blind, paralyze, or confuse the enemy before launching precision-strike or other sorts of conventional attacks.

- The Chinese clearly concentrate on the *offensive dimension of information warfare*. Even in discussions about the U.S., more attention is paid to the offensive capabilities that the PRC can emulate than to how to defend against U.S. IO and IW initiatives against China. This is in direct contrast to the U.S., where the primary focus, particularly with respect to strategic IW, has tended to be on defense.

- When the Chinese did discuss defense, they focused primarily on *low-tech countermeasures to frustrate the high tech advantage of the U.S.* There were very few discussions of protecting C4 networks, for example. By contrast, it was clear the Chinese were particularly impressed with the camouflage, deception, operational security and other techniques employed by the Serbs against the U.S. and NATO.

- While the Chinese are clearly in the very early stages of developing a theory of IW, they are even less sure of how to modernize their military – forces and organization alike – to suit the changing nature of warfare. Among the strategic paths the Chinese feel they can adopt are:
  - Approach the problem in *Stages* – modernize current forces in Stage I, then develop RMA and IW forces in Stage II.
  - Adopt a *Transcendental* approach – ignore modernization of current forces and begin preparing RMA and IW forces for the future.
  - Employ a *Comprehensive* Strategy – adopt a strategy that simultaneously pursues modernized forces for today and RMA forces for tomorrow.

VI. Implications

In the near term, there are at least two tasks that need to be accomplished. First, Chinese language specialists should explore the untranslated literature for the validity of these findings. As noted in the introduction, we are well aware of the biases inherent in assessing themes based primarily on translations of unclassified writings. Second, we believe it may be a matter of some urgency to determine whether Chinese writings on information warfare and information operations did in fact take a dramatic turn in 1999, or whether the changes we detected were simply an aberration based on unique political and military circumstances.

In addition to these rather short-term implications for further analysis, we believe there are policy indications inherent in our findings. In particular, we believe that the U.S. should:

- Recognize the Long Term Competition. It is clear, particularly in writings on IW and the character of future warfare, that most Chinese defense analysts perceive the U.S. to be their principal long-term competitor. Further, while in many respects China lags behind the United States in military capability, the Chinese believe this is, potentially, a transitory state of affairs. In this context, we believe the U.S. should recognize that the relationship between the U.S. and China will always have a competitive dimension. Over the longer term, we believe this has several implications – the simplest of which is that the U.S. be sensitive to IW/IO and other RMA-related developments in the PRC.

- Take advantage of the Leader-Follower Dynamic: China's unusual position of wanting to both emulate the United States and develop asymmetric capabilities against the United States offers the U.S. an opportunity to exert considerable influence over the directions of Chinese IO/IW thinking and information technology R&D. This dynamic is more complex, we suspect, than simply a leader-follower relationship. There is a tendency, among Chinese analysts, to openly acknowledge the United States as a leader in both technology and conceptual development. The Chinese not only lag behind, but openly recognize that the PLA is following the U.S. in the application of information technology to warfare, rather than pursuing an alternative path. This tendency is complemented by a surprising degree of credulity in following U.S. exercises and demonstrations. This was certainly the case with regard to experiments and training exercises (i.e. the Army's digitization experiments), as well as in Kosovo where the Chinese believed the U.S. could not have made the mistake of targeting the Chinese embassy.

It should be possible to use these observations to shape Chinese thinking on IO and IW, as well as to influence their Research and Development strategies more generally. Rumored success of particularly effective IO/IW weapons or techniques, reportage on the conduct of Advanced Warfighting Experiments, and a number of other techniques might be able to influence Chinese actions. Given a decision to adopt a long-term strategy, planks of the strategy are clearly available.

- Taking advantage of bureaucratic differences: At several points over the course of this report, we hypothesized that one explanation for Chinese actions in some area and inaction in others might derive from splits in the Chinese bureaucracy. If true (and we believe there is enough circumstantial evidence to make the possibility very real), there may be ways to exploit these divisions to U.S. benefit. Clearly, before taking any action, a detailed and focused needs to be done by experts in the Chinese Government and the PLA.

- Learning from U.S. Failures: Although it might technically be beyond the purview of this study to suggest that the U.S. engage in very serious analysis of any C4, ISR, and information operations failings in Kosovo, we would urge that such a study be undertaken. It is very clear that the Chinese (and presumably other potential competitors of the U.S.) are analyzing Serbian successes – and U.S. failures – intensively.

- IW Focus: Chinese writings focus on the tactical and operational level of ground combat, with particular attention to using IW and IO in an offensive manner during the preliminary phase of a military operation. When discussed, defensive aspects of IO and IW almost always focus on low-tech, passive activities at the lowest tactical levels (e.g. camouflage, radio discipline). We believe the failure to address other areas will, over time, create military vulnerabilities that can be exploited. The lack of attention to IO and IW at the strategic level, overlooking the importance of joint operations, failing to address what could be vulnerabilities of new command and control networks, and focusing on using IO and IW primarily during a preliminary "phase" of a confrontation are all potential vulnerabilities that could be exploited.

- Intelligence Indicators: We believe there are several clear indicators that could signal a more dedicated Chinese IO and IW effort. Among these are:
  - Indicators of Organizational Change: As mentioned in the text of the report, some of the most serious thought given to information warfare related to how China's military bureaucracy may need to change in order to compete effectively. As with other bureaucracies, particularly those based largely on patronage, China's defense establishment will likely find change exceedingly difficult and perhaps impossible. If, however, such change is effected, it could mark a significant step toward real defense modernization.
  - Changes in the education and training of soldiers and leaders: While technology may be the "long pole in the tent" for many western militaries, the Chinese recognize that the training of their soldiers and the education of their officer corps are precursors to the

development of any information-based military capability. The unclassified writings indicate clearly that the Chinese have started moving down this road with the development of a number of institutes that explore the relationship between information and military capabilities. Intelligence agencies should watch closely how the Chinese evolve.

Sun Haicheng, Yang Jie, and staff reporter Zhang Guoyu: "Let Information Warfare Training Rule the Training Sites: Practice and Reflections from the First All-Army Collective Training Session for Division and Brigade Chiefs of Staff in Information Warfare Theory"

Jiefangjun Bao in Chinese 13 Jul 99 p 6

Document ID: FTS19990808000796
Entry Date: 08/08/1999
Version Number: 01

[FBIS Translated Text] Editor's Note: Some people say that the war in Kosovo showed the basic form of high-tech warfare for the first part of the next century. Whether that assertion is proved correct or not, the things that the war in Kosovo left for the consideration of our military, as it prepared to step into the next century, will be deep and all-encompassing issues.

Recently, with the approval of the General Staff Headquarters, the first all-army collective training session for division and brigade chiefs of staff in information warfare theory was conducted by the Communications Command Academy. The division and brigade chiefs of staff who came from various units throughout the army used the war in Kosovo as a guide to seek a frame of reference against an even broader backdrop, strengthening our military's focus in preparing for military struggles and making an effort to take the training activities of our University of Science and Technology for National Defense to a deeper level. Through 40 days of collective training, the chiefs of staff arrived at a common understanding: There will probably never be another war like that in Kosovo, which caused every soldier to have an intense awareness of the compelling nature of computerized warfare. The key in meeting future wars is to launch comprehensive information warfare training for our military, letting information warfare training rule the training sites!

1. In the nine short years between the Gulf War and Kosovo, the US military has accelerated its effort to get information warfare out of the laboratories and into the battlefield. The pattern in Kosovo may not be repeated, but the outlines of information warfare can now be clearly discerned.

NATO's Painstaking Construction of the Information Warfare Battlefield [subhead]

Ye Zhisheng (Unit 83013): Although there was less than 10 years between the Gulf War and Kosovo, progress in the computerization of warfare has developed very rapidly. During the Gulf

War, people were only able to analyze and predict information warfare through scattered battlefield phenomena, but as of the war in Kosovo, information warfare has now become a combat activity that is intensely confrontational, and it not only permeated the war from start to finish, it also played a leading role during the war.

As early as a year prior to the use of force in Yugoslavia, NATO (North Atlantic Treaty Organization) had started its information warfare outposts. The US military used various military satellites to conduct close surveillance and monitoring of the Federal Republic of Yugoslavia (FRY), as well as using various other high-tech means to carry out continuous electronic and spy reconnaissance, collecting intelligence information.

The Balkans are a target the United States has been aiming at for a long time. A favorable battlefield information environment and a computerized battlefield network with powerful functions provided an enormous convenience for the battlefield information operations of the NATO forces. The information infrastructure whose construction began during the Cold War played an extremely important role during the war. The NATO headquarters and the C3I systems distributed among the various NATO member countries used digitized equipment to network command, control, communications, intelligence, monitoring and reconnaissance, and other network systems into an organic whole so that the land-based, sea-based, sky-based, and space-based combat platforms and various categories of personnel were able to exchange combat information in real time, as well as sharing various information resources, forming a multidimensional information space to support the various combat activities. On the highly transparent computerized battlefield, NATO was able to acquire the various static and dynamic combat information it required, as well as transmitting and processing it in near real time, basically achieving visual command and control, and improving the precision and real-time nature of the information acquired.

Li Xiaoxing (Unit 54854): Following the Gulf War, there has been a rapid expansion of the depth and breadth of the application of information technology in the military arena, and the computerization of weapons and equipment has also developed from single weapons to weapons systems, as well as going from the strategic level deeper to the tactical level. A variety of diverse computerized weapons systems now occupies the stage of high-tech local warfare. In December 1998, the United States and Britain launched an air attack against Iraq dubbed "Desert Fox," and computerized weapons have now become the mainstay force on the battlefield. During the war in Kosovo, NATO's computerized weapons systems -- centered around precision guided weapons -- were in nearly total control. The satellites, early-warning aircraft, reconnaissance aircraft, and helicopters covering the sky in the Balkans, the reconnaissance ships on top of and beneath the surface in the Adriatic and Mediterranean seas, the radar and intercept facilities deployed on the ground in Bosnia-Herzegovina, Albania, Macedonia, and other countries around the Federal

Republic of Yugoslavia, as well as the ground reconnaissance personnel who penetrated Kosovo, formed a complete information reconnaissance and early-warning system for the NATO side. The missiles and guided bombs launched from the land-based, sea-based, and sky-based platforms, which were the only means used directly by NATO in combat to kill, destroy, and damage enemy targets, were hard-kill computerized weapons systems. The soft-kill computerized weapons, psychological warfare weapons, and graphite bombs, etc., played an extremely important role in the war. Using its superior computerized weapons systems, NATO carried out air-strike combat against the Federal Republic of Yugoslavia in which information warfare played a lead role, taking a critical further step in the transition of mechanized warfare to computerized warfare.

Liu Xinsheng (Unit 36101): From a military perspective, the computerized combat operations by NATO against the Federal Republic of Yugoslavia achieved relatively ideal results. There were essentially four steps in NATO's combat formula: one was to use information reconnaissance operations to acquire precise intelligence information on strike targets, two was to use hard [weapons] to destroy or paralyze the command and control system and the air defense system of the Yugoslavian people's army, "plugging the ears, gouging out the eyes, and paralyzing the body," three was precision combat led by electronic warfare to attack the various military, economic, transportation, energy, public opinion media, and even daily-life targets in the Federal Republic of Yugoslavia, and four was to carry out damage assessments using airborne and ground photography and observations to determine the next bombing targets and make corrections. The NATO cycle proceeded in these four steps, with information operations permeating the entire process. NATO also actively carried out information blockades, using technical and deterrent means to cut off the FRY's channels for acquiring information from the outside world and keep the military and civilians there from acquiring critical information.

FRY Seeks Symmetry Amid "Asymmetry" [subhead]

Feng Yihe (Unit 83351): During the Gulf War, the US-led multinational forces destroyed Iraq's information systems at one stroke in a relatively short period, creating a "lopsided" situation so that there were no operations involving information countermeasures, nor were we able to get a clear look at the outlines of battlefield information operations. The traditions and courage of the Yugoslavian military and civilians in resolutely opposing aggression represent an important guarantee for securing victory in war, but correct combat leadership and an intense awareness of information countermeasures were the basic factors that put a stop to the 78 days of wild and indiscriminate bombing by NATO.

Prior to the war, the Federal Republic of Yugoslavia expected that the opponent would inevitably resort to "air strikes" supported by information warfare, and only by stepping up their preparations to counter the enemy's information warfare would they be able to counter the enemy's "air strikes." Conducting combat preparations with a focus on information warfare, constructing information warfare positions based on the requirements of the information warfare battlefield, and studying and practicing information warfare tactics became the center of the combat preparations by the FRY military.

Zhao Zhongxi (Unit 54773): To deal with the enemy's complete space-time, high-intensity electronic reconnaissance and air strikes, the FRY made full use of the civil-defense works, bunkers, and underground arsenals that had been built since World War II, as well as civil architecture and caves, etc., constructing an underground battlefield in which they "hid to counter reconnaissance, using a combination of concealment and attack." To deal with the enemy's high-precision, pinpoint strikes that came in waves, they adopted deployment that divided the whole into parts, combining action with waiting and actively constructing a ground battlefield in which they "moved to avoid destruction" and "used the ground to control the air." To deal with the characteristics in which the enemy's firepower systems were in a position of absolute superiority while the network systems were vulnerable to attack, they made full use of the power of a people's war, widely mobilizing the people to take part in combat and opening up a network counterattack battlefield.

Based on the overall design of the information warfare battlefield, the FRY first constructed information warfare positions. For example, they focused on the flaw in the enemy's electronic reconnaissance systems in which "the target can be seen clearly, but it is hard to distinguish what is real from what is bogus," constructing a large number of fake radar positions, fake artillery positions, and fake tank positions, etc., using the fake positions to conceal the real ones. To deal with the flaw in the enemy's precision guided weapons in which they go out of control when they encounter smoke, they piled up old car tires and weeds, etc., near important targets, setting fire to them at the appropriate time before an enemy attack to create smoke barriers and jam the attacking weapons. To block detection by the enemy's thermal imaging systems, they relied on industrial heat sources that put out heat year round to construct "thermal cover" positions, covering tanks, artillery, and other equipment deployed nearby so that it was not detected.

Huang Lingfang (Unit 32833): The FRY was also studying the characteristics of information warfare by NATO prior to the war, studying and practicing tactics to avoid the enemy's strengths and attack their weaknesses. As early as following the outbreak of the war in Bosnia-Herzegovina, the FRY was concentrating on studying the performance characteristics of the Tomahawk cruise missiles used by NATO in bombing the Serbs and ways to bring down the US F16 fighters. In particular, following the conclusion of the US and British "Desert Fox" operation, the Yugoslavian army had sent personnel to Iraq to learn from their experience, creatively formulating a complete set of information warfare tactics that were in keeping with the realities in their own country. For example, there was the tactic of "avoiding strikes" by not turning on or seldom turning on their air defense radar, keeping NATO's precision guided weapons from finding their targets. There was the tactic of "hooking the fish" in which folded corrugated steel, etc., was used to decoy the radar, misleading the attacking missiles and aircraft. There was the "hide and seek" tactic in which they took advantage of the blind zones and dead angles in the operational orbits and dead air of the NATO reconnaissance satellites, shifting during the windows of opportunity. Based on characteristics such as the mixed formations of the attacking NATO weapons and their multi-echelon attacks, they used "relay intercept" tactics in which they mixed the deployment of radar with different modalities and used the cross-deployment of weapons with different ranges to lay ambushes along the attack routes, switching on the radar suddenly, performing intercept by firepower at different levels, and concentrating the fire of the weapons, achieving remarkable combat success in controlling the air from the ground.

Acquiring an Accurate Frame of Reference While Learning From Others [subhead]

Shen Huiqin (Unit 32822): With the conclusion of the war in Kosovo, like the Gulf War pattern, the Kosovo pattern will not be repeated. In the next war we will see some new wrinkles, perhaps based on the Kosovo pattern. However, the Kosovo battlefield and the lead role played by information countermeasures has sounded the alarm bell of the times for us. Information warfare will dominate future battlefields. Faced with this challenge, we must get away from the conventional methods of industrial-age mechanized warfare that we are familiar with, update our combat concepts, and launch energetic studies of information warfare and comprehensive training in information warfare so that such training occupies a leading position in our military training system, using training in information warfare to push the scientific and technical training throughout the military to new heights!

1. The computerized battlefield in Kosovo has reflected the light of wisdom of the scientific and technical training of our military forces. Scientific and technical training for the military does not represent a patch on the original training model, but should represent a redesign of the training grounds based on the battlefield.

What the Main Focus of Scientific and Technical Training for the Military Should Be [subhead]

Zhao Chunyan (Unit 81167): Our military really did not get a later start than the West in studying information warfare, but we have been very slow with regard to training breakthroughs. The basic reason for this is that the question of the "position" of information warfare training has still not been resolved, so we cannot create a situation in which information warfare training plays a leading role. Is it possible for our military units, with their relatively backward equipment, to have information warfare training play a lead role?

For information warfare training to play a lead role is not a transition that relies on human will, but is an objective requirement of the development of warfare. This is what we mean by the common expression "train the way you are going to fight." The shift of mechanized warfare to computerized warfare requires that military training open up a new phase in which information warfare training is a principal entity. This collective training session shows that our military has already taken a great step forward in incorporating information warfare training into the military training system.

However, we should also note that irrationalities in the training content, system, and structure have kept information warfare training from truly becoming the mainstream of our military training. At present, information warfare training is in a "do-as-you-please" situation in which the content is not systematic, the operations lack order, there are no assessment standards, and management lacks regulations. To make information warfare training into a main theme in our scientific and technical military training, we cannot just make it an add-on to the original training framework, but should have information warfare training become a principal part of the content of military training in our army, thereby forming a new generation of military training contents and systems in which information warfare training is a primary focus. To do this, we must formulate as quickly as possible a new generation of training rules, centered around information warfare training and including training programs, training courses, assessment standards, and organizational management, etc., using regulations to standardize the overall development and orderly operation of information warfare training.

Follow the "Fast Lane" Rule in Computerized Training [subhead]

Duan Jianmin (Unit 53023): Determining the content of information warfare training is a front-end process in starting up information warfare training. It should include four parts: One is basic information warfare theory, including information warfare concepts and characteristics, the current status and development trends in information warfare, and an overview of our military's theoretical research on information warfare, etc. Two is basic information warfare techniques, including information acquisition, transmission, and processing, countermeasure techniques (information reconnaissance and counter-reconnaissance, jamming and anti-jamming, computer countermeasures, code-breaking and security, and destruction and destruction countermeasures), etc. Three is information warfare tactics, primarily including counter-reconnaissance, anti-jamming, destruction countermeasures, and tactics to attack aircraft, cruise missiles, and command centers, etc. Four is information warfare command and control, including command and control principles and modes, command and control preparation and implementation, command and control countermeasures, and command and control information security and safeguards, etc.

Zhang Ming (Unit 51036): Because information warfare training involves considerable contents and different specialties, when implementing the training, depending on the subject, we can follow the principle of selecting what is primary and what is secondary, how much time should be allotted, how deep the grasp of the subject should be, and how tough the assessment standards should be, planning scientifically and making flexible determinations. For example, training for senior staff offices should focus on basic command and control knowledge, while that for specialized information units such as those involved with communications, reconnaissance, electronic countermeasures, and radar, etc., should focus on basic information warfare techniques and basic counter-reconnaissance, anti-jamming, and counter-destruction tactics, and infantry, armored, and artillery troops, etc., should focus on basic information warfare tactics, particularly tactics to attack airplanes, cruise missiles, and command centers.

In applied information warfare training, the focus must be on seizing information warfare supremacy, altering our traditional specialized technical training courses and striving to blend traditional specialized tactical exercises with the general backdrop of information warfare. For example, air-defense units should develop special technical training, applied training, and tactical training with regard to how to use battlefield information systems to acquire intelligence regarding enemy attacks, how to improve their own counter-reconnaissance, anti-jamming and counter-destruction capabilities, how to improve position-fixing reconnaissance to attack aircraft, cruise missiles, and the enemy, how to jam the enemy's target acquisition and their command and control systems, etc., developing special technical training, applied training and tactical training, and studying technical, tactical, training, and command and control methods.

With regard to special information warfare demands, special targeted training can be conducted, such as information security testing, message encryption, and guarding against information attacks, etc., as well as attacking computers, jamming satellites, and paralyzing information networks, etc.

Establish a Training Organization Approach Suited to Information Warfare Training [subhead]

Sheng Linguo (Unit 55051): With advances in information processing technology and network technology, there have been revolutionary changes in information warfare training methods. The individual, base, and network orientation of such training, and its integration, will become new characteristics. With regard to the organization of training, we should stress the development of the information warfare capabilities of the individual soldier, that is, enhancing the training of the individual combat elements and platforms of the various specialized services and arms to improve the individual information warfare capabilities of the various combat elements and platforms. On the basis of individualized training, we should implement base-oriented training, with the navy, air force, and army each setting up their own information warfare training centers (bases), establishing an appropriate information warfare environment, and conducting training in keeping with the demands of information warfare. In particular, units at the division and brigade level and up should all establish information warfare training bases in keeping with their level and specialties.

Ding Yuming (Unit 81562): Information warfare training should follow the path of network-oriented training, achieving the integrated utilization of battlefield resources, network resources, and training resources so that all the elements undergoing training can participate in a manner that transcends regions, times, and airspace, changing information warfare training from a static, linear approach to a dynamic, non-linear mode. Through a network approach, specialized training in information warfare can obtain the support of a joint-operations environment and training models. The training of non-information warfare specialized forces can also use the network approach to obtain the help of special databases and models. The "Networked Information Warfare Training System" developed by the Communications Command Academy makes the most of this advantage, assisting the division and brigade staff officers with a large "information warfare database," providing advanced training modes and methods for the study of information warfare and enhancing the sense of freshness, a feeling for the time-domain, a sense of dynamism, and the sense of time constraints.

What Is Important Is Completely Revamping the Training Methods [subhead]

Xu Yong (Unit 56016): In designing computerized training sites, we need to get the troops to have a real feeling and understanding of the computerized environment. During our current collective training classes, a multimedia approach with a large number of integrated video, optical, and audio effects was employed to vividly depict the mysteries of information warfare, simplifying a complex process, clarifying chaotic things, making mysterious effects real, and enhancing the workability of information warfare training. Using modern simulation techniques is an important way to give information warfare a real-combat orientation, and the key is to establish computerized battlefield models, develop dynamic mathematical models of information warfare based on chaos theory, and continue to update and optimize the databases that support the simulation.

Virtual reality is the optimum approach for information warfare training. This can raise the difficulty and the level of the training, developing the creative capabilities and potential superiorities of the training subjects. With the realities of our military in mind, we should adopt a two-pronged approach, popularizing virtual reality training in our joint (combined) training centers or bases and, at the same time, modifying the methods used at the training sites for units at the division or brigade level or lower to create virtual information warfare training sites and enhance the effectiveness of information warfare training.

1.To turn the "blueprints" for carefully designed training sites into reality, there are quite a few hard and tight "bottlenecks" in our way, so each step forward will require a greater effort than in the past.

Just Who Should Be In Charge of Information Warfare Training? [subhead]

Yang Delin (Unit 52884): The basic reason why, at present, the overall program for information warfare training for the units is incomplete and leadership at the macro-level is not forceful is that it is not clear which departments are responsible for organizing training. There are those who equate computerization with command automation, believing that since command automation is the bailiwick of the telecommunications departments, they should also be in charge of information warfare training, and the other departments need not participate. Then there are those who believe that information warfare is special training for the information-related arms and services, so it is sufficient if it is managed by the arms and services which specialize in information, and it is not necessary for the general departments to meddle. In fact, in high-tech warfare, the battlefield focus is to seize information superiority, so the battlefield operations of all the arms and services should be centered on this. This means that information warfare training should cover all the arms and services, running through the entire training process, so we must establish a training leadership system in which the senior military officers are in command, which is under the unified administration of the general departments, with the arms and services sharing in the management.

Having the senior military officers in charge means we must affirm the leading position of computerized training, create a leadership core, and establish the main emphasis of the training. Unified administration by the general departments means that an information warfare training department should be established jointly by the training, communications, reconnaissance, and other departments to formulate a uniform information warfare training program, coordinate regarding information warfare training sites, organize information warfare training sessions, conduct information warfare training assessments, and create a joint force. Shared management by the arms and services means that, based on an overall plan, each of the departments in the various arms and services should establish training classes for their own arm or service, formulating training programs and standards, organizing and writing training courses, bearing responsibility for training the instructors, and doing a good job of organizing information warfare training for the specialized units in their own arm or service.

How to Resolve the Problem of Training Materials and Equipment [subhead]

Xue Benping (Unit 32360): Information warfare training is a brand new training course, and without training materials and equipment there is no way to get started. However, we cannot just sit and wait for the higher-ups to allocate the materials and equipment, but should make an effort to be self-sufficient, using indigenous methods and taking an integrated approach involving improvement and innovation, leasing, purchasing, development, and allocations. The military units can join with the research departments in tackling the tough problems, embedding information technology into current training equipment and materials, or installing chips in traditional weapons and equipment to achieve programmable controls, automated aiming, and smart evaluations, getting training to change from a unitary mode to an integrated mode, and changing from numerous attacks to more accurate attacks. The laser simulation cruise missile tracking system developed by a certain unit seems to have resolved the problem of not being able to train with real equipment. In addition, as needed, it is also possible to lease or purchase training equipment, teaching materials, software and multimedia courseware that is not under the unified allocation system, as well as general purpose information equipment and materials which the units urgently need and which is already on the market. The relevant operational departments in the general headquarters should arrange for the educational and research institutes to focus on the development of the simulation equipment and the associated high-performance software urgently needed by the units, as well as speeding up the commercialization of research results, batch-production design, serialized production, and unified allocation, ensuring that the results of scientific research related to information warfare are transformed into training capabilities as quickly as possible.

Information warfare training is a must. Getting an early start gives us the initiative, while a late start will inevitably put us in a passive position. When training money is lacking, we can ask offices at higher echelons for some, squeeze some out of office expenses, or take a bit from production expenses. When there are not enough training materials and equipment, we can conduct training on a priority basis, doing a good job with our reserves of technology and talent.

How to Build Training Sites [subhead]

Tan Benhong (Unit 53203): Without being involved in cyberspace or in the information environment, it is meaningless to expect high returns from information warfare training. Accordingly, the construction of information warfare training sites is an important link that cannot be neglected.

The establishment of a training site is not simply a site issue. The first thing to be resolved is the approach to networked training. Only when the approach is understood will there be a way out.

First, we must use network technology to link the microcomputers of the staff departments and those of the battalions, companies, and squads, creating local-area networks (LAN) and turning them into training sites on information-warfare tactical networks and information warfare command and control networks. By modifying the cable television system in one's home unit, a closed-circuit television network can be established, making it into a learning site for information warfare tactics and theory. Second, provide training sites for the troops and training centers for military officers, outfitting them with information infrastructure and automated management equipment so that they become information warfare tactical training sites for the soldiers and information warfare interior exercise sites for commanders and staff officers. With regard to a large, integrated training center, in keeping with computerized battlefield requirements, we can reestablish operational agencies, reclassify operational areas, and reestablish site elements to create an integrated training base which brings together command and control systems, electronic countermeasures systems, intelligence acquisition systems, target positioning systems, fire control systems, and outcome evaluation systems into an integrated whole, making it into an information warfare rotational training base and integrated exercise base for the units under the various arms and services.

The key in setting up networked training sites is the development of software systems. The various systems must all have a uniform software operating environment and interface standards and the size of the site must be planned scientifically to meet the information warfare training needs of the various arms and services, with the quantity not being important as long as it is effective.

Where Will the Skilled Training Organizers Come From? [subhead]

Cui Haichen (Unit 81389): Information warfare training is not simply moving guns, artillery, and vehicles back and forth, and relying on loud voices alone won't work, nor does the traditional approach of having "one unique skill" do much good. Information warfare training calls for innovative skilled individuals. What we mean by innovative skilled individuals are instructors who are well versed in information warfare methods, who understand information warfare techniques and tactics, and who understand information warfare equipment. The various units should carry out surveys of command automation specialists and technicians, information specialist cadres, and soldiers with an aptitude for computers, then on that basis transfer personnel for collective training, turning them into "greeters" at the front door of the units as they initiate information warfare training. At the same time, they should rely on the officer training centers and training bases to conduct group training for the instructors who have the "four know-hows," concentrating on study of the characteristics of information warfare instruction and instructional methods, bringing traditional training and information warfare training "in line" with each other as quickly as possible. In addition, they should establish information warfare training centers to conduct rotational training for commanders and staff personnel at various levels.

THIS REPORT MAY CONTAIN COPYRIGHTED MATERIAL. COPYING AND DISSEMINATION IS PROHIBITED WITHOUT PERMISSION OF THE COPYRIGHT OWNERS.

Wang Baocun, Research Fellow and Senior Colonel, Academy of Military Sciences: "A Preliminary Analysis of Information Warfare"

Beijing Zhongguo Junshi Kexue [China Military Science] No 4 in Chinese 20 Nov 97 pp 102-111

Document ID: FTS19980329000129
Entry Date: 03/29/1998
Version Number: 02

[passage omitted]

2. Primary Forms of Information Warfare

There are many forms of information warfare: Divided up in terms of time, we have peacetime information warfare, information warfare in times of crisis, and wartime information warfare; divided up in terms of its nature, we have offensive information warfare and defensive information warfare; divided up into levels, we have national information warfare, strategic information warfare, theater information warfare, and tactical information warfare. In addition, several other distinctions can be made.

(1) Command and Control Warfare

Command and control warfare is the core element of information warfare, and its essence is: To maintain one's own command and control capabilities and, at the same time, weaken or undermine the command and control capabilities of the opponent in order to ultimately seize "information superiority." Up to now, the primary objective of combat operations has been to concentrate troops and weapons, wipe out enemy personnel, and destroy the enemy's equipment. In the future, the primary objective of combat will be to destroy the enemy's command and control system, particularly its critical nodes.

Command and control warfare is suitable for various phases of a war. Conducting this kind of combat relies on three points: One is that modern military technology, equipment, and combat operations demand a continuous supply of large amounts of information, and if they are cut off from information, military units and their equipment may lose their "life" and "soul" and find it difficult to move at all; two is that information and intelligence systems which widely employ new and advanced technology are vulnerable and have many weak points that are easily attacked; three is that, with advances in science and technology, the performance of information and intelligence systems is constantly improving. It goes without saying that these three points mean that, in command and control warfare, attacking and defending are of equal importance.

The attack targets in command and control warfare are: Attacking the enemy's information transmission systems, particularly the system's weak links and critical facilities, to undermine the enemy's command and control capabilities, rendering the enemy commanders incapable of understanding the battlefield conditions, losing "information superiority," and ultimately submitting because of "information starvation" resulting from their inability to obtain information. Because the enemy's information transmission systems are extremely large and complex, various methods should be used when conducting attacks, not only engaging in "hard kills" but also "soft kills," so that, at the least, the enemy's information flow "arteries" are severed.

Because one's own information and intelligence systems will inevitably have weak points that are vulnerable to attack, to ensure that one's own side maintains effective command and control capabilities, command and control defenses must be tightly organized and implemented.

(2) Intelligence Warfare

Intelligence warfare is an important form of information warfare. Its goal is to ensure that one's own commanders obtain the intelligence they require in a timely manner and to see that the opponent's commanders have no way of obtaining the intelligence they require. Modern intelligence warfare requires that intelligence be used directly in combat operations and that it be used in attacking enemy targets and conducting damage assessments. This is primarily because the sensitivity and reliability of detection devices and equipment is increasing daily and there is a continuous increase in their quantities and varieties, so they are now capable of providing intelligence information to the weapons' fire control systems on a real-time basis.

There are significant differences between intelligence warfare today and that of the past, and this is primarily reflected in the use of the intelligence. In the past, intelligence was primarily used by commanders in assessing the enemy's deployment, position, and intentions, and information was collected to prevent sudden attacks and to help the commanders in formulating combat plans. Today, with respect to the degree of detail and the accuracy, the intelligence supplied by intelligence information systems far surpasses that of systems of the past. At present, through the use of his own systems, a commander can observe the activity of the opponent's armored units on the battlefield and can pinpoint the location of each enemy tank, and therefore he can attack with accuracy. The role of modern intelligence has changed from preparing for combat to control of the battlefield, and the primary recipients of the intelligence have changed from being only high and mid-level commanders to high, middle, and low-level commanders as well as weapon operation groups or weapon systems.

The primary method of collecting intelligence in the future will be various detection devices and equipment distributed over the entire combat space, including ultra long-range detection devices (primarily space-based sensing devices), long-range detection devices (such as unmanned aerial vehicles outfitted with various kinds of radar and electronic information collection equipment), fixed detection devices (such as acoustical sensors, gravimetric sensors, and biochemical sensors, etc.), and weapons detection devices (such as infrared radar, reflection radar, and ranging radar, etc.).

Intelligence warfare is divided into offensive and defensive intelligence warfare. Offensive intelligence warfare refers to the use of a variety of methods, primarily involving detection devices and equipment with various effective distances and resolution power, and the real-time acquisition, transmission, and use of intelligence information. Defensive intelligence warfare includes two aspects: One is camouflage and deception measures, including the use of smokescreens, anti-radar coating, and maintaining radio silence; two is the use of various methods to attack the enemy's intelligence information systems.

(3) Electronic Warfare

Electronic warfare is a series of activities to ensure that one's own side can fully utilize the electromagnetic spectrum while simultaneously preventing the enemy's military from using it. It is an electronic struggle conducted to weaken and undermine the use and effectiveness of the enemy's electronic equipment and to ensure the normal and effective operation of one's own electronic equipment. The widespread use of modern microelectronic technology in various weapons and equipment has resulted in a close correlation between the performance level of various weapons systems and C4I systems and the degree to which they employ microelectronics technology. Along with the further modernization of weapons systems, the amount of electronic technology in weapons and equipment also continues to increase, and it constitutes an ever-increasing proportion. According to U.S. military statistics for 1989, in that fiscal year the proportion of the total cost of related weapons and equipment accounted for by electronic equipment purchases was: 22 percent for naval vessels, 24 percent for military vehicles, 35 percent for aircraft, 45 percent for missiles, 66 percent for satellite systems, and 88 percent for command systems, respectively. By 1996, the proportion of electronic equipment costs in these kinds of equipment had increased 8-17 percent. In information warfare, one of the keys to seizing the battlefield initiative is establishing electromagnetic superiority. If electromagnetic superiority is lost, sea and air supremacy will inevitably be lost, and ultimately the battlefield initiative will be lost. Electronic warfare has become an important element in demonstrating one's own superiority and restraining an opponent, and has become an important form of combat to seize the battlefield initiative and win victories in war.

In information warfare, electronic warfare is made up of three parts. The first is electronic offensives. In an electronic offense, electronic jamming, electronic deception, or directed-energy weapons are employed to undermine, destroy, or take advantage of the enemy's ability to use the electromagnetic spectrum. The second is electronic defense. Electronic defense refers to protecting one's own ability to use the electromagnetic spectrum, that is, comprehensive protection of one's own related personnel, equipment, and facilities. When conducting electronic defense, various protective systems should be used to jam the enemy's target acquisition and attack systems in order to prevent the enemy's military forces from destroying one's own systems and wiping out one's own forces. The third is electronic warfare support. This kind of support refers to the use of related systems, under the direct control of the battlefield commander, to search for, intercept, and fix the position of the enemy's electromagnetic energy radiation sources and to identify actions the enemy may take which will directly threaten one's own side.

(4) Psychological Warfare

Psychological warfare may be targeted at the masses, and it may also be targeted at military forces. It is "the transmission of selected information and information carriers to foreign military listeners (or viewers, readers) to first influence their feelings, motives, and objective reasoning abilities, and ultimately to influence the actions of their government, organizations, and groups." When conducting psychological warfare, in general one should transmit true and reliable information.

The primary methods for conducting psychological warfare are: Television and radio propaganda, distributing leaflets, and sending email, etc. Psychological warfare can be used to exert psychological pressure on the enemy's officers and men, cause the enemy's ruling clique to waver in their determination, destroy the enemy's morale, cause splits within the enemy's camp, and weaken the enemy's combat capabilities, achieving the objective of "an army which gives up without a fight" or paying a small price for a major victory.

Psychological warfare is an important form of information warfare whose purpose is to alter the mental state of the enemy's military and civilian personnel. It has three features: One is the focus on the overall situation in the war. When conducting psychological warfare as an organic part of war activities, one must keep an eye on the overall situation in the war, have a unified plan, coordinate well, focus on the features of the social, military, and civilian situation, select the right opportunity, and have a firm grip on the crucial points. Two is the full employment of advanced technology. To meet the needs of modern warfare and expand the impact of psychological warfare, both combatants will fully utilize modern science and technology to improve their means and operational methods in psychological warfare, thereby improving their results. Three is to take advantage of contradictions. Surveys and understanding of the ideological situation in the enemy's military and political circles must be strengthened, gathering and taking advantage of all the internal contradictions among the enemy's top leaders, between higher levels and lower levels, and between various military units.

(5) Cyberspace Warfare

Cyberspace is the sphere of computer activity or actions on a network or in a system. Cyberspace warfare primarily includes information terrorism, "semantic attacks," and "punk shadowing," etc. Information terrorism is activity by terrorists using computer network systems. Information terrorists may be computer enthusiasts in general or enemy computer specialists. They can use computers or radio signals reflected from satellites to detonate explosives placed in other countries. Under normal circumstances, these terrorists do not attack groups but individuals, particularly the military and political leaders of enemy countries. Their methodology is: To seek out records and material on their attack targets that is on a network, then conducting extortion by threatening to make the records public, or altering the contents of the records. "Semantic attacks" are not the same as "hacker warfare." "Hacker warfare" may cause computer systems to malfunction or shut down, whereas systems which have been subjected to "semantic attacks" not only continue to operate as usual, they also appear to be operating perfectly normally. The objective in "semantic attacks" is to "ensure that the answers coming from the system do not conform to reality," and the method used is to transmit false data or bogus signals to the computer system's detection devices. "Punk shadowing" refers to computer "punks" who use information systems to track the activities of certain personnel, including important military and political figures. With continued improvement in the information infrastructures of various countries, more and more personal computers are connecting to international and domestic information networks, so "punk shadowing" will become easier to perform.

(6) 'Hacker' Warfare
This is a brand new form of conflict. "Hackers" generally refers to users of computers and computer programs. This method of combat primarily involves the use of harmful software programs to destroy or take advantage of the enemy's information systems. Its functions are to: Completely paralyze the enemy's electronic information systems; force periodic shutdowns in the enemy's information systems; pilfer the enemy's information and data on a large scale; cause random errors to appear in the data; and input bogus messages and extract data to be used in extortion. The methods generally employed are computer viruses, logic bombs, Trojan horses, and "sniffer" programs. At present, the greatest threat is from computer viruses, of which there are more than 12,000 varieties.

There are three primary modes for carrying out computer virus attacks: One is spatial insertion, that is, using a computer virus weapon to irradiate a certain unprotected reception and processing system in the enemy's electronic countermeasure systems, or C4I systems with an electromagnetic radiation signal carrying a virus. Two is insertion into a network/node, that is, inserting the virus directly through certain weak networks/nodes in the enemy's electronic systems or C4 I systems. This method requires that one be able to come into direct contact with some of the enemy's equipment. Three is insertion during the development phase, which primarily refers to implanting a virus in the computer hardware, operating system, maintenance tools, or diagnostic programs through a certain path during the development period of the electronic equipment, with the virus lying dormant for a long time and waiting until after the equipment is delivered, then being triggered by certain specific conditions.

(7) Virtual Warfare

Virtual warfare is using a realistic combat environment created with virtual reality technology and the simulated exercise combat operations conducted with the enemy. Its function is to achieve the goals of war without using a single gun or a single soldier. The four following circumstances all constitute virtual warfare:

One is using virtual reality and computer imaging technology during the course of the war to construct images of the enemy's supreme commander and have him issue statements that are not conducive to the conduct of the war, such as having him declare through his homeland's television system that, for various reasons, hostilities with the enemy have ceased and all military forces are being withdrawn.

Two is using virtual reality technology to create "virtual military units" or "virtual fleets," having the enemy observe from satellites or radar that these combat forces are coming from a certain direction, while in fact "real military units" coming from another direction are making preparations to launch an attack.

Three is to create religious holographic icons to shake up the enemy psychologically. In the future, when the U.S. engages in combat with Iran, they plan to display a holographic image of Allah in the air, having this lifelike Allah urge the Iranian soldiers to surrender. U.S. Army psyops units conducted experiments in this area during the peace-keeping [mission] in Somalia. Related materials provide the following report on this: On 1 February 1993, at a place 15 kilometers west of Mogadishu in Somalia, a sudden sandstorm came up, and at the same time a 150-200 meter high holographic icon of Jesus Christ appeared amid the murky swirling sands. Seeing this, quite a few of the American peace-keeping soldiers fell to their knees to pray.

Four is for the military leaders of both sides to engage in "simulated warfare" before engaging in real combat. That is, both sides will enter the major elements of all their combat capabilities into a computer program and engage in a contest along the lines of a computer-simulated opposing-forces exercise. The side that is confident of victory can invite the opponent to view this "simulated warfare," demonstrating to them that resorting to armed force will inevitably result in defeat. Looking at the present situation, there is not a great likelihood that this kind of "simulated warfare" will occur, because it is not possible that both sides will provide the real circumstances and data on the performance and quantities of their respective weapons, or on their combat methods and reconnaissance, intelligence, and camouflage systems.

(8) Economic Information Warfare

Economic information warfare refers to information warfare whose purpose is to undermine the enemy's economy, including economic information attacks and economic information blockades.

Economic information attacks refers to "information offensives" undertaken through computer network systems by a country, an organization, or an individual to undermine another country's economy. The more a country has been computerized and networked, the more vulnerable it is to information attacks. For example, the financial and trade systems in the United States have already basically achieved computerized networking, and more than 60 percent of America's medium-to-large companies have global interconnectivity. For this reason, America's economic system is extremely vulnerable to information attacks. According to statistics, because of economic information attacks, an average of one dollar is lost for every $1000 worth of business done on the Internet. The losses to international credit card companies because of credit card errors come to $1.41 out of every $1000. The economic losses to the U.S. as a result of information attacks come to as much as $10 billion annually. "Hacker operations" are an important form of economic information attacks. In 1988, a "hacker" broke into a bank in Chicago through a computer network, wiped out accounts and transferred funds overseas, resulting in a $70 million loss to the bank. In August 1995, a criminal in St. Petersburg, Russia, used a computer to make off with $400,000 from the First National City Bank of New York.

An economic information blockade refers to cutting off the enemy country's links to external economic information, and its effects are determined by the enemy country's degree of reliance on foreign trade. The more a country relies on import and export trade, the greater the damage to its economy. In the case of countries which have just begun to establish links between their own economies and the world economy, an economic information blockade may have a serious impact on their economic development. The methods for carrying out economic information blockades are: Blocking electronic information exchanges between the enemy country and other countries, and shutting down the international computer networks going to the enemy country; severing the underwater and land-based wire line communications between the enemy country and other countries and jamming air and sky-based radio communications; suppressing individual communications and preventing communications between third parties and the enemy country.

(9) Strategic Information Warfare

In 1995, the Rand Corporation organized 170 experts from political, military, industrial, and academic circles for a six-month study of the issue of information warfare, coming up with the new concept of "strategic information warfare." Strategic information warfare is using cyberspace to influence strategic military operations, a "form of confrontation" that may result in serious damage to a country's information infrastructure. In making a comparison between strategic information warfare and information warfare in general, other than the fact that the combat methods are the same, the major difference is that the former has more potential adversaries, a wider range of attack targets, and greater strategic significance. Potential adversaries may include a given country, and they may also be a private-sector organization, an international criminal group, or even an individual. The attack targets include information, the information infrastructure and other strategic targets in the military, political, economic, and social areas.

Strategic information warfare has four features: One is that the cost of launching a war is low. Compared to high-tech weapons systems, the manufacturing costs of computer viruses and other such information warfare weapons are very low. From another angle, because the information network systems in cyberspace are increasingly complex, they have weak points which are vulnerable to attack, providing conditions which are conducive to carrying out effective information attacks. Two is that some of the traditional boundaries have become blurred, and this includes some of the boundaries between society, government, and other organizations, the boundaries of national sovereignty, the boundaries between public interests and private interests, the boundaries between military and commerce, and the boundaries between strategy, campaigns, and tactics. Three is that it has become more difficult to gather strategic intelligence. For a variety of reasons, it is very difficult to use traditional intelligence collection means to meet the challenges of information warfare and determine intelligence collection targets. At present, intelligence collection targets have expanded from countries to non-governmental organizations, international criminal groups, and hostile elements, so new methods must be used to launch intelligence collection efforts. Four is that combat early warning and attack assessments are more difficult. An information warrior may use information warfare weapons to launch a strategic attack at lightning speeds, then very quickly return to his original working state, and generally there are no advance indicators of an attack, so it is very difficult to issue a warning. It is very difficult to evaluate attacks, because at present there is no way to distinguish among an attack, an accident, a malfunction, and an unintentional external intrusion, etc.

(10) Precision Warfare

Precision warfare is the combat approach of conducting precision strikes against enemy targets which results in very little collateral damage. The reasons that it belongs to the realm of information warfare are primarily: First, the information-technology content of weapons used in this kind of combat is high; second, conducting this kind of combat requires a battlefield with a high degree of transparency. Using weapons systems which contain a large amount of information technology makes it possible to attack and destroy enemy targets with a high-degree of precision at very long ranges. Once a battlefield is transparent, friendly forces can obtain information very quickly, accelerating the process cycle of "clarifying the situation, making a decision, and taking action" and more accurately seizing combat opportunities, thereby ensuring that combat operations are more precise and lethal than before.

When conducting precision warfare, one should: Quickly clarify the enemy's defensive center of gravity, the "points that determine victory or defeat" and other critical points; unless it is absolutely necessary, one should avoid engaging in a "decisive battle" that results in heavy losses on both sides; distribute the deployment of troops, only concentrating ones forces for short periods of time to destroy critical targets; use long-range precision firepower as much as possible, particularly when neutralizing the enemy's defensive weapons.

Units conducting precision warfare should possess the following capabilities: There should be a perfectly clear understanding at all times of the position of subordinate units (elements), as well as of the deployment circumstances of the enemy forces' combat systems; the capability of analyzing and processing the large amount of battlefield information received, as well as providing it to the battlefield commanders in real-time in a usable form; each unit (element) should have voice frequency and digital communications equipment that performs reliably at all times; the ability to destroy all targets within range of organic and support weaponry; the ability to sustain combat operations for long periods of time without relying on external support and secure communications lines.

3. Features and Combat Principles in Information War

(1) Primary Features of Information War

Compared to war during the industrial age, particularly mechanized warfare, information war, information warfare, and war in the information age have the following characteristics:

1. Motives for War Are Becoming More Complex

During the industrial age, the fundamental motive for war was a struggle for economic gain under the cover of political struggles, primarily striving for territory, resources, and other economic gains, and often ending with the occupation or recovery of territory and the acquisition of resources. In the information age, the struggle for economic gains is still the primary cause leading to war. In addition, because of increased exchanges and ties among various countries and among the various international and domestic political forces, there are more conflicts among nations, nationalities, and social groups stemming from political, diplomatic, spiritual, and cultural clashes, resulting in increased religious and national contradictions and the internationalization of terrorism, violence, and drug smuggling. These contradictions and clashes are intricate and complex, and are not only the direct source of "sub-war operations," they are also a primary cause leading to war. As for those who launch information war, in addition to nations and national groups, they also include terrorist organizations, drug trafficking groups, industrial and commercial enterprises, religious groups, criminal gangs, and other groups, because they can likewise possess the various means of conducting information warfare, such as computer viruses, mass media, and large-scale lethal weapons, etc.

2. Goals of War Are More Limited

In information war, generally one is not pursuing "ultimate goals" such as occupation of the enemy's entire territory, annihilating the enemy's military forces, or causing the enemy to "totally" surrender, etc. This is primarily because to do so would lead to both combatants, particularly one's own side, sustaining heavy losses that would be difficult to accept, and thereby result in an intense antiwar mood among the people. In the information age, communications, television, and radio broadcast systems cover the globe, and each country's reconnaissance and monitoring satellites are flying over the battlefields every minute of every hour, so the battlefield conditions, particularly the casualty situation, will be reported by television in real time. With the battlefield being monitored by the watchful eyes of the people, those directing the war must impose strict controls on the course and goals of the war.

3. Wars Are Short in Duration

Because of developments in computers, electronic communications, and satellite technology, the speed at which war progresses will be accelerated, and the duration shortened. The fundamental cause leading to this situation is: Increased precision and range of weapons and equipment and the establishment of the digitized battlefield, resulting in combat operations being conducted in real time with precision strikes.

Real-time operations refers to having an immediate response and countermeasures for situations that occur on both sides on the battlefield, primarily including real-time target identification, real-time command, real-time maneuvers, real-time strikes, real-time damage assessments, and real-time support, etc. The benefit to this approach is that what formerly took several hours or longer to accomplish on the battlefield can be compressed to several minutes or even several seconds, so that decisions and the course of operations are nearly synchronized, thereby greatly shortening the course of war.

Precision strikes refers to using smart weapons with "eyes, ears, and brains" to hit the target 100 percent of the time, even hitting a specific part of the target. The sensors on these weapons are capable of picking up all the direct and indirect target information that can be used, including acoustic, radio-wave, visible light, infrared, and laser [information], and even odors and gases, with computers differentiating and analyzing this information, then once again automatically recognizing, tracking, and attacking the target, so "no rounds are wasted." In information war, the main target for precision strikes is the enemy's command and control systems, because this way one can quickly cause the enemy to submit and bring the war to an end.

4. Less Damage in War

Information warfare has one other major feature, which is that the amount of damage is limited. Damage in war falls into two categories, one being effective damage and the other being collateral damage. Effective damage is necessary damage that is directly related to achieving the objectives of the war, while collateral damage is unnecessary damage that is not directly related or is totally unrelated to achieving the objectives of the war. In wars during the industrial age, there was a great deal of this kind of collateral damage, which was primarily caused by the level of development of military technology at the time. In war during the information age, that is, in information war, the amount of collateral damage will be held to a minimum. First, because the transparency of the battlefield is great and both combatants have large amounts of information, not only will it be possible to avoid sustaining heavy casualties from surprise attacks, it will also be possible to prevent unnecessary direct face-to-face firefights that cause heavy losses. Second, because both sides are only attacking those targets that it is necessary to attack to accomplish the mission, units from both sides are only exposed in the battlespace for short periods of time and sustain fewer casualties. Furthermore, to a certain extent, information warfare is also "precision warfare," and "precision warfare" requires "precision" in detecting, attacking, and destroying targets, as well as in damage assessments, so it will not result in collateral damage tens or hundreds of times greater than the "necessary damage" as was the case in the carpet bombing and area fire during the industrial age. Finally, the goals of information warfare are limited, it is not all-out warfare to kill the enemy, so in general both sides in the hostilities do not engage in desperate, decisive battles among massive forces.

5. Larger Battlespace, Reduced Troop Density

Foreign military forces believe that "Developments in military technology will result in a continuing expansion of the depth, fronts, and heights of the battlefield, and the development trend in warfare is to have fewer soldiers in an expanded battlespace." One of the salient features of information warfare is the large battlespace and the small troop density.

There are two reasons for the expansion of the battlespace: One is that even small-scale information war requires the deployment throughout the world and in space of satellite monitoring systems, airborne warning and control systems (AWACS), joint surveillance and target attack radar systems (J-Stars), and unmanned aerial vehicles (UAVs), etc., to collect, process, and transmit large volumes of information; two is that computerized and networked weapons can hit various targets from very long ranges, turning today's three-dimensional ground, sea, and air battlefield into a five-dimensional ground, air, sea, space, and electromagnetic battlefield. For example, a surface warship or submarine anchored a thousand miles away can be used to launch ballistic missiles and cruise missiles to attack enemy tanks, and through multiple mid-air refueling, stealth fighters can be used to attack enemy command and control centers. With advances in C4I systems and further improvements in the performance of weapons, the battlefield commander's observation range continues to expand, and his ability to control the battlespace is continually being enhanced. At the same time, with the mutual overlapping of the various armed services in the battlespace, the commanders of joint operations can make use of the weapons systems of the various services, hitting various targets throughout the entire scope of the battlefield.

The gradual reduction in battlefield troop density is one of the inevitable trends in the development of war. During World War I, the force deployment per square kilometer was as high as 404 soldiers; during World War II, this was 36 soldiers; during the Arab-Israeli war in 1973 this fell to 25 soldiers; by the time of the Gulf War, there were only 2.34 soldiers per square kilometer, and on the digitized battlefields of the future, the troop densities will be even smaller.

6. Perfectly Transparent Battlefield

The "fog of war" has always been a difficult issue causing problems for battlefield commanders, but when it comes to digitized troops conducting information warfare, the battlefield is transparent. Some analysts believe that the degree of transparency of the digitized battlefield will be "an order of magnitude greater than during the Gulf War." In information warfare, sensors on the front lines and space satellites will transmit the various circumstances continuously to computers, as well as displaying the intelligence information and pictures and images on the command post computer screens in real time. All the combat personnel on one's own side can get these images
simultaneously, thereby seeing the positions and the posture of the hostile and friendly forces as well as troop concentrations and movements, etc., very clearly.

The U.S. military is making a tremendous effort to establish the digitized battlefield, and the goal is to make the battlefield transparent. Once the battlefield has become digitized, it will be possible to transmit intelligence from theater, army, and division headquarters, etc., in digitized form to the brigades, battalions, companies, and even to individual combat vehicles, so that the commanders at all levels can share information; combat vehicles will be able to report their positions while they are maneuvering, and the computer screens of all their combat vehicles will be able to display the position parameters of the hostile and friendly forces at any time. The digital compression technology that will help make the battlefield transparent can be used to expand the enemy detection range, improve information processing capabilities, and transmit the battlefield conditions silently and with excellent text and images to the users accurately and in real time.

7. Struggle for 'Information Superiority' Extraordinarily Intense

U.S. military theoretician John Aquilar [as transliterated] points out, "The simplest and the most accurate definition of information superiority is understanding all the enemy's circumstances and, at the same time, keeping the enemy from understanding your situation." He also states, "Information superiority will become the primary factor affecting the progress and outcome of war." In information warfare, under most circumstances, what the majority of the combatants are handling is not materials and energy but information, because information has supplanted materials and energy as the key to achieving victory. The formation and use of a military unit's fighting capacity, as well as effective combat command, rely primarily on the collection, processing, transmission, control, and use of information. A superior brigade becomes "a blind and deaf target" as soon as it loses "information superiority," sinking into a passive predicament and taking a beating. If an inferior army gains information superiority, it can seize the initiative on the battlefield. Because future strategic, campaign, tactical, and combat operations all depend on and center around information, the struggle to seize information superiority will be extraordinarily keen and intense, and furthermore will permeate the entire course of the war. Specifically, seizing "information superiority" has the following advantages: The "fog of war" surrounding your side can be dispersed, while making the "fog of war" around the enemy heavier; your side's command effectiveness can be improved, fully grasping and taking advantage of combat opportunities; the hit rate of your weapons can be improved, greatly enhancing their combat effectiveness.

8. Unprecedented Increase in the Degree of Combat Integration

An unprecedented increase in the degree of combat integration is another salient feature of information warfare. First, there will be a high degree of integration in ground, sea, air, and space combat, and this will not only be manifested in large-scale wars, it will be the same in small-scale clashes. Second, it will not be easy to distinguish the dividing lines among operations by different service arms. For example, the weapon that destroys an enemy tank may not be a tank or an antitank weapon from your army, but a "smart" missile launched by an air force aircraft or naval vessel. Third, theater combat operations will be integrated. Because digitized military units will be able to grasp information in real time and operate swiftly both day and night, it is just as Sullivan said, "The dispersed theater campaigns that arose from the industrial age no longer exist, and taking their place are integrated combat operations conducted throughout the entire theater." Fourth, the lines will become blurred between combat at the strategic, campaign, and tactical levels. This is mainly because the precision and power of computerized and networked weapons provide an effective way to achieve the objectives in war quickly, and at times it will be possible to achieve strategic and campaign objectives without using a large force. Finally, various combat systems such as combat units, combat support units, combat logistical support units, and various combat functions such as battlefield intelligence, command, control, communications, strikes, and damage assessments, etc., will be linked to form an organic whole. Coordinated operations among the various combat units in this whole will serve to increase combat effectiveness several times over.

9. High Demands On, Great Degree of Difficulty In Combat Command

Because of the wide variety of weapons and equipment used in information warfare, the instantaneous changes in battlefield conditions, the accelerated tempo of combat, and the dramatic increase in the volume of information, the demands on combat command have not diminished, but have increased and become more difficult. This is primarily reflected in four areas: One is that command must be in real time or near real time, otherwise military operations will be hindered and one becomes passive. The focus of real-time command is on "seizing and controlling the battlespace," restraining the enemy military force with respect to speed, time, and responsiveness and thereby ensuring that your actions are always a half or a full beat ahead of the enemy's. Two is command during maneuvers. This is because the battlefield of the future will be very fluid and units will always be on the move, so it will be very difficult for a commander to set up a fixed command post. Three is that one must adopt vertical and horizontal command methods. This means transmitting information from level to level among higher and lower echelons to effect vertical command, and carrying out horizontal command by the direct and indirect transmission of information at the same level during controlled marches, air defense early warning, and other such activities. During fire support and other such activities, a combined vertical and horizontal command method should be adopted. Four is that coordination is complex. In information warfare, many service arms are involved and the battlespace is large, so the horizontal coordination tasks are extremely demanding.

10. New Aspects to Massing Forces

In information warfare, the ancient military principle of massing one's forces still applies, but its features have changed.

First, the focus of massing forces has changed from the tactical and campaign level to the campaign and strategic level. In wars during the industrial age, it was first necessary to concentrate ones forces at the tactical and campaign levels in order to achieve a continuous and cumulative combat effect, eventually achieving the campaign and then the strategic objectives. In information warfare, with the massive use of precision-strike and stealth weaponry, campaign or strategic objectives can be attained through one or two firepower strikes, so there has been a change in the focus of the concentration of one's forces.

Second, the essence of concentrating one's forces has changed from concentrating troops and weapons to concentrating firepower and information. In the future, it will not be necessary to concentrate troops to concentrate firepower. Long-range precision guided missiles, fighters, bombers, and C3I system networks can hit and destroy all the targets in a theater. It is not necessary to have a concentrated deployment of the various long-range strike weapons to conduct concentrated assaults on a target. To achieve the effective use of concentrated firepower, a great deal of information must also be concentrated, otherwise there is no way to acquire, track, and destroy the targets. Compared to concentrating troops and weaponry, the advantages of concentrating firepower are: One can avoid concentrating ones forces and thereby giving the enemy a useful target to attack; one can take full advantage of long-range, powerful, high-precision, high-tech weapons; and there is greater surprise, responsiveness, and stability.

Finally, there is a shift from concentrating mainly ground and air power to concentrating ground, sea, air, and space power. In information warfare with a powerful enemy, it will not be possible to attain superiority over the enemy and achieve victory by concentrating ground and air power alone. Therefore, the common approach to concentrating ones forces will be to concentrate air, ground, sea, and special operations capabilities throughout the theater and, with support from space-based combat systems, carry out joint campaign-level operations.

11. The Enemy's Effective Strength Is Not the Main Target of Battlefield Strikes
In wars during the industrial age, only by continuing to destroy the enemy's effective strength could one bring about a change in the relative strength of your own forces and the enemy's forces, alter the war situation, overcome the enemy's will to resist, and seize victory. In information warfare, because of the links among the various weapons platforms, the various combat and support systems, and the various forces involved, as well as because of great enhancements in the systematic features of the battlefield force structure, the battlefield force structure is developing into an organic combination of effective strength and automated, intelligent weapons and equipment systems, and the amount of one's effective strength is no longer the primary indicator of relative strength. Confrontation and contests between systems has become a prominent feature of information warfare. Obviously, under these circumstances, only by carrying out a damaging or destructive attack against the critical links making up the enemy's combat system, destroying his battlefield structure, paralyzing his combat system, and fundamentally weakening the enemy's ability to resist, will one be able to effectively alter the relative strength of your forces and the enemy's forces and thereby win victory in war. Therefore, one's effective strength is no longer a principle target in battlefield strikes.

(2) Combat Principles in Information Warfare
When carrying out information warfare, in general one should abide by the following principles:

1. The principle of "decapitation." So-called "decapitation" is "attacking the enemy's head, not his body." This principle requires: First attack the enemy country's command authorities, the joint staff, theater headquarters, and the unit headquarters at various levels; destroy all the enemy's information media -- telephones, the radio frequency spectrum, cables, and other transmission means; keep the enemy from using third party communication systems, including communication satellites.

2. The principle of "blinding." This principle requires that one "first destroy the enemy's sensors and other detection devices and equipment, not wipe out enemy personnel," rendering the enemy blind and deaf. The specific features include: Destroying or jamming the enemy's electromagnetic emission devices and radio-frequency stations, using soft and hard means to neutralize the enemy's automatic homing weapons, electronic jamming devices, and air defense

firepower; neutralizing or destroying the enemy's passive sensors, using smart weapons to destroy the enemy's wide spectrum video observation instruments, using lasers to irradiate the enemy's optical tracking instruments, and bombing the enemy's radio-frequency (RF) receivers; preventing third-party satellites and ground-based sensors from providing information to the enemy.

3. The principle of battlefield transparency. There should be continuous, tight, multispectrum monitoring and observation of the enemy to ensure that one understands the situation on every part of the battlefield clearly, maintaining "transparency throughout" regarding oneself. This principle requires that one do a good job of three things: One is using various equipment and methods to penetrate clouds, darkness, and the part of the earth's surface that can be penetrated to observe the battlefield, understanding the changing situation at all times; two is ensuring that one is capable of fully receiving sensing data from remote units, not transmitting the information to fragile communication nodes and distributing the data directly to the individuals doing the firing; three is ensuring that battle damage assessments are speedy, comprehensive, and accurate, avoiding as much as possible wasting resources on decoys or targets that have already been destroyed.

4. The principle of quick response. You should ensure that the decision-making cycle for your units is always ahead of the enemy forces and faster than the enemy forces; the process of firing, maneuvering, then firing again should be carried out even faster so that the enemy always finds himself in a situation of being hit, surprised, then being hit again. The most important thing in achieving this is that those providing information should be totally devoted to the mission, capable of providing the required information at any time or ahead of time.

5. The principle of survival. This principle primarily refers to enhancing the survivability of the command and control system, and the primary measures that may be adopted for this are: Use multiple-node, multiple-route, and multiple-frequency systems, and also employ dispersed deployment; employ mobile satellite receiving devices and change their deployment position frequently; bury optical cables between fixed firing positions and emit deceptive signals from secondary nodes; formulate a backup communication plan and make sure there are redundant communication circuits; continually upgrade information technology and equipment, maintaining superiority in C4I technology.

THIS REPORT MAY CONTAIN COPYRIGHTED MATERIAL. COPYING AND DISSEMINATION IS PROHIBITED WITHOUT PERMISSION OF THE COPYRIGHT OWNERS.

Su Enze: "A Personal Look at the Innovations in China's Military Theory"

Jiefangjun Bao in Chinese 15 Dec 98 p 6

Document ID: FTS19990120001559
Entry Date: 01/20/1999
Version Number: 01

[FBIS Translated Text] In two decades of reform and opening, China's whole strategic concept has been "to use the first decade as good preparation for the next." And the progress in military theory can also be divided into two corresponding stages. The first decade was the preparatory stage for the new military theory, in which new ideas guided by an "orientation toward modernization, the world, and the future" sprang up like bamboo shoots after a spring rain. And the last decade has been the growth period for the new military theory, in which we began to form a conceptual framework for a new military theory that is characterized by meeting the challenge of the global revolution in military affairs and pursuing the Central Military Commission's strategic principles for the new era.

Clarity of Theory Is the Greatest Clarity

The conceptual framework for the new military theory has evolved in five areas:

1. The setting and premise for the growth of the new military theory: the revolution in military affairs. We face the challenge of the global revolution in military affairs; the radius of the earth has "shrunk," with the dimensions of the battlefield "multiplying," and the lines between traditional strategy and tactics, armies, navies, and air forces, and the forward and rear areas gradually blurring. Thus, of the three factors in the revolution in military affairs, military theory, which stands with weaponry and military organization like the three legs of a tripod, also had to undergo revolutionary change.
2. The backbone and core of the new military theory: high-tech warfare. The Gulf War was known as a "World War 2.5" -- not a typical war, but rather an information war. This shows that the high-tech warfare model of modern warfare is neither the traditional conventional war nor nuclear war. While it remains mechanized, it is beginning to show signs of being information warfare. Thus, modern armed forces are now in transition from being mechanized to being information-intensive or "smart."
3. The pull and precursor for the new military theory: information warfare. In correspondence with the "information age" and the "knowledge economy," warfare is also becoming ever more characterized as "information war," "knowledge war," and "smart war." Information warfare has two major pillars: One is the computer-backed "cyber war" that is promoted by

the West, and which is growing like wildfire due to web space and hypothetical or simulated realization technology. Another is the "strategy war" based on the human mind that is undergoing profound development in the East, and which is in a new stage because it has assimilated modern technology. Their bottom line is "thought-dimension warfare," or, in the final analysis, a test of thought-dimensional quality.

4.The key and essence of the new military theory: "the Chinese model." Due to China's national conditions, our defense- and force-building means must accord with "the Chinese model," or carrying our traditions forward and maintaining our distinctions, instead of blindly following the developed nations. We have to act creatively in terms of China's realities, taking shortcuts, and pursuing sound strategy, to achieve "more, fast, good, and economical" results.

5.The aim and outlook of the new military theory: "the world pattern." When we stress theory with Chinese characteristics, taking a different path, the goal that we are aiming at is international quality, or "the world pattern." In other words, while our battle strategy is in accord with "the Chinese model," our quality accords with "the world pattern." Thus, we must pay attention to getting onto an international track, being good at assimilating the latest and best human developments, to build effective and efficient national defense and armed forces.

Clear Policies Are the Hardest To Set

Within the framework of this new military theory, we still must act in line with China's national conditions, to form policy thinking for theoretical research in areas such as equipment, personnel, training, force building, and battle strategy.

1.Equipment. While China's weaponry has long been Chinese-made, it has certainly not yet broken free from the "copied" model. After many setbacks, we have finally come to the realization that we need to pursue the "demand" principle, using combat requirements as our criteria, developing what we can develop, buying what we can buy, and researching what we can research, for a transformation from "fighting whatever kind of war our equipment will allow" to "acquiring whatever weapons are required to fight." And investigation has led us down the path of secondary criteria, forming a cutting edge, several generations coexisting, and upgrading by echelon, displaying our advantages of combining men with machines, coordination and supplementation, quality training, and meticulous maintenance, and achieving victory by sudden strikes with a "killer mace," which is fully capable of enabling Chinese weaponry to near international quality faster.

2.Personnel. Future wars will be based on talent, with personnel training playing a leading role. Former U.S. Air Force Chief of Staff Flugleman says that "the quality of the man determines the fate of the air force." The standards for military personnel quality should be high, or the "top talent" and the "elite of the race." The knowledge structure for military personnel should be optimum, or a composite and smart model. And the personnel quality model should be good, or a progressive-tower model of knowledge, ability, quality, and awareness. And we need to engage in "talent engineering," or "full-course cultivation" such as attracting outstanding youths, optimizing our recruitment structure, controlling our training model, rationalizing our training levels, choosing the right priorities, adhering to our appointment system, performing our primary mission, evaluating technical titles, accumulating academic knowledge, keeping our key technicians, combining hiring with management, raising our pay and benefits, improving our support forces, and embellishing our personnel image.

3.Training: The core of the new training is to establish an awareness of "strengthening our military through S&T," clarifying that S&T is the number one productive force, military might is made up of S&T, war readiness is the S&T assimilator, and combat is the joint S&T battlefield.

The training urgency is "eliminating illiteracy" and "cultivating enthusiasts," to raise the S&T quality of our officers and men. We need to eliminate scientific, mathematical, academic, and information illiteracy, cultivating science, math, academic, and information enthusiasts.

The training priority is training commanders. Our military leaders should stand in the front ranks of the revolution in military affairs, being familiar with everything without being bogged down in details, and knowing the history of war well without being mired in models.

And the heart of training is all-round versatility, so that our officers and men can face the information shock with neither "information fear" or "information worship."

1.Development methods. Systematic thinking is the fast track to methods of development. Faced with the modern warfare "confrontation of system against system," development methods must stress "systematic overall planning" and "top-level design." Since scientific proof is the basic means for development methods, it is only scientific proof that excludes the factor of subjective will that can draw up a good blueprint.

Building a quality force is the overall requirement for methods of development. The general trend in all countries in today's world is to take a series of steps such as raising a global awareness, tapping historic potentials, summing up combat experience, rectifying professional arms, making strategic adjustments, and intensifying military theory, to raise armed forces quality.

1.Battle strategy. Combat effectiveness is the key to battle strategy. This means that new equipment must be combined with personnel and translated into combat effectiveness.

Evaluating the information battlefield is a new battle strategy task. Since mastery of information is growing ever more important in modern warfare, besides evaluating the materiel and capabilities of both sides, it is also necessary to evaluate the information status.

Finding the way to win is the crux of battle strategy. In this respect, I would stress the following: We must master high technology, with our high-tech research not being shallow or following ruts. We need to develop new ideas, with our military thinking being more emancipated. We need to produce new data, with our theoretical research producing experiments and data. We need to change to a new structure, with the value of action being a systematic return to advance planning and organization. We need to be innovative, since the victors know that that the basic matter in battle strategy is cultivating talent. And we need to endeavor to plan well, since it takes a long time to sharpen a sword for one day of battle.

We must focus on flexible thinking, since S&T is all true, but S&T inferences are certainly not. This means that an over-consideration of pure technology at times can obstruct thinking, deviate from combat needs, and lower the awareness of security. If we can change our perspective, our horizons will be broader. Richard Hurd said that, "in the history of warfare, while there were fewer great ideas than great generals, they had a much larger impact."

Finding the Problem Is the Greatest Discovery

We need to find problems in order to improve, to make greater advances. So what are the major current research problems in China's military theory?

It is too low-tech. Faced with high-tech warfare, military theory that does not stress high technology lacks a "core," and is nothing but a "shell." So we are subject to problems such as shallow high-tech studies, a lack of high technology in our military academies, and a lack of an S&T foundation among our military personnel.

It is too showy. Some ask, are we not using many computers? Leaving aside the fact that high technology is certainly not confined to computers, as to computers alone, they are now used mostly for show, which is subject to flaws such as an overuse of information ideas, exaggeration of computer functions, obstruction of military integration, and the cultivation of a formalistic academic style. It is understood that, while the integrated technical performance of China's current automated command hardware is ten times better than that of the US military in the late 1970's and early 1980's, its effectiveness is less than one-tenth that of the US military at that time. That 100-fold gap gives much food for thought!

It is too traditional. While Chinese military thinking is now largely emancipated, faced with the growing S&T standards and rapid advances of the times, it is far from adequate. Our military theory is hampered by much traditional thinking, which can be seen in its slowness to keep up with the latest change and over-dependence on "encyclopedias," famous experts, and well-known works. In which respect, the United States that seems to be at the peak has a greater sense of crisis, calling the military revolution a "pentagon palace coup." So it is going all out to encourage creativity among its officers and men, to pave the way for "out-of-the-box thinking."

It is short on experimental data. While it has long since been established that military theory is the "hardest science," there is another aspect to the matter, or that military theory is essentially social science, which is subject to "easier input" because it needs no laboratory equipment, but only data, investigation, and research to be raised to a philosophic elevation. So the easy input but hard output is a matter that military theory must stress. The key to which is in-depth investigation and research, doing experiments and data analysis.

It has a slow practice cycle. US military theory is also characterized by a fast practice cycle; not only in all of its "operational laboratories" but also in its unit organization and exercises, it stresses fast practice. New weapons and thinking are tested, with the unsuitable parts changed. In other words, of the three factors in the military revolution of weaponry, military theory, and military organization, a fast practice cycle is the only way to achieve combat effectiveness and keep up with the times.

THIS REPORT MAY CONTAIN COPYRIGHTED MATERIAL. COPYING AND DISSEMINATION IS PROHIBITED WITHOUT PERMISSION OF THE COPYRIGHT OWNERS.

Yang Minqing: "Facing the Future Information War"

Jingji Cankao Bao (Economic Information Daily) in Chinese 15 Oct 99 p 5

Document ID: FTS19991129001723
Entry Date: 11/29/1999
Version Number: 01

[FBIS Translated Text] If someone were to say that national news organizations and their employees will be among the troops on the battlefield of the future, and that equipment such as electronic computers will serve as weaponry to attack the enemy, there would be some who would consider it a tale out of "The Arabian Nights." However, these nevertheless are the facts in information warfare (IW). Moreover, these facts have been corroborated by IW in regional wars fought in recent years under high-tech conditions. Precisely for these reasons, people need to gain a fresh understanding of national communications media in the IW of the future.

NATIONAL INFORMATION WARFARE AND NATIONAL DEFENSE INFORMATION WARFARE

"Information warfare" refers to a face-off in the field of information between opposing parties, which is reflected primarily in a fight to gain the initiative as far as information resources and control of the production, transmission and processing of information, so as to damage information-based public opinion on the enemy's side. All this serves to create favorable conditions for checking enemy power and/or winning a war. IW revolves primarily around the information of the two sides, and is waged by means of processes such as understanding, analysis, policy-making, commanding, and getting feedback (all of which are based on information), and by means of information systems and computer networks.

IW may be divided into two fields. The first is national information warfare, and the second is national defense information warfare. In national IW, the goal is to seize the upper hand in regard to the acquisition and utilization of all the information among the two nations. National IW embraces intelligence warfare, diplomatic warfare, commercial warfare and strategic psychological warfare. The primary tools for waging national IW are news agencies, television, radio, newspapers and magazines, books, communications networks, and diplomatic activities (all of which can serve to represent the nation), as well as various types of reconnaissance, espionage and eavesdropping activities.

In national defense IW, the goal is to seize the upper hand in regard to the acquisition and utilization of all the information among the armed forces of the two sides. National defense IW embraces intelligence warfare, electronic warfare, command and control warfare, and psychological warfare, etc. The primary tools for waging national defense IW are automated command and control systems, electronic warfare systems, and broadcasting systems, as well as various types of reconnaissance and eavesdropping facilities. National IW embraces national defense IW and is broader in its scope. National IW embraces more fields than does national defense IW.

A race to control the information space and a fight for information resources are the primary hallmarks of IW. Two main forms of warfare are included in IW: the non-violent contest in peacetime, and the armed contest under actual war conditions. National defense IW is more acute and intense during wartime. However, national IW runs throughout both peacetime and wartime.

THE AGE OF INFORMATION WARFARE IS ALREADY UPON US

Under high-tech conditions, the struggle between two parties in a war in the field of [media] communications has already evolved into a new form of warfare--a form that is an important component part of IW.

The role and function of IW have become more and more prominent and more and more important in two recent wars--the Gulf War and the air assault by NATO on the Yugoslav Federation. The following point is generally recognized not only by military experts, but also by the broad mass of the people of the world; namely, that now IW is occurring all the time, in social life all over the world. The age of IW is already upon us.

In the war in which NATO carried out an air assault on the Yugoslav Federation, one could see very clearly the fight between national communications media over public opinion. Before the war, NATO, led by the U.S., used the mainstream media in the Western nations to greatly distort the real nature of the impending war, seeking to exert a widespread psychological effect on the standpoints and attitudes prevailing in international society. They extensively reported the so-called "bloody atrocities" of the Yugoslav Federation's Serbian nationality against the ethnic Albanians, and they sought by every possible means to imprint numerous images of "scenes of slaughter" that were "dripping in blood" on the minds of people. Thus they tried to lead people, (particularly Western people), to believe that the war launched by U.S.-led NATO was motivated by a desire to protect Western values, and that the war was a "just operation" designed to punish the "butcher" Milosevic.

In the early stages of the war, U.S.-led NATO waged war simultaneously on the two main battlefields--the military battlefield and the battlefield of the heart. The mainstream media of the

Western nations extensively reported the "huge effects" accruing from the large NATO force bearing down on the border and the repeated bombing, trying to make the Yugoslav Federation surrender very quickly. When a supposedly "legendary" NATO F-117A and other aircraft were shot down, what was reported extensively by the mainstream media of the Western nations was rather the "legendary experience" of the troops who were sent on the rescue mission. At the same time, NATO dispatched a psychological warfare detachment and made use of a variety of modern communications methods. They set up an airborne broadcasting station. They broadcasted a large number of programs to the battlefield and scattered numerous propaganda materials over the battlefield, with as many as 11 million propaganda leaflets alone being distributed. In addition, they also adopted a number of other measures, such as the intentional fabrication of news, luring people by the promise of material gain, and extensive use of the Internet to prosecute the fight for the information initiative.

In this war, U.S.-led NATO, in order to achieve its desired IW goals, flagrantly violated international law and carried out premeditated surprise guided missile attacks on the Yugoslav Federation's national news organizations and China's embassy in the Yugoslav Federation. U.S.-led NATO murdered dozens of employees of news organizations from other countries who had standpoints that differed from NATO's, including three Chinese reporters. This type of atrocity had been very rarely seen in prior wars.

THE NEW CHARACTERISTICS OF NATIONAL COMMUNICATIONS MEDIA

A number of scholars who have visited the U.S. in the past maintain that every important report in the U.S. mainstream media has a clear strategic intention, and that not one of them is a "random shot." These reports have long-term goals as well as near-term goals. One could say that each report is linked to another and that relatively few are arbitrarily subjective and reflect mere personal volition. The more a report directed against the enemy or against another country is stated in a positive manner, or the more a report reflects a so-called "righteous reaction" on the Internet, the more it should lead us to heighten our vigilance, because a report that is communicated in this manner generally has a definite strategic purpose. To speak thus is not by any means to "see the enemy behind every bush", nor is it by any means an example of "weakness lending wings to rumors."

Compared to the traditional communications media of the past, national communications media under high-tech IW conditions have special characteristics in the following four main respects:

1) National communications media have risen from their past subsidiary strategic role to take a dominant strategic role. This transformation has led to a qualitative change in traditional communications media. Communications media now have a prominent role and a prominent

function in wars. Moreover, communications media also appear to be more important in peacetime now. The goal of the war of the future will shift from territorial expansion and economic pillaging to a fight for the information initiative. While it is true today that wars in some regions of the world are still triggered by factors such as territory and resources, it is nevertheless also true that the war goals of the hegemonic countries have already undergone some change. The hegemonic countries believe that information has already become a political and diplomatic weapon, and that if used properly, it can serve to shake the foundations of a nation's political power. Thus, communications media that pertain to IW have risen from their past subsidiary strategic role to take on a dominant strategic role. Now we can see all the time, right in front of our eyes, that the information battlefield serves as an organic whole that combines the bloodless battlefield with the bloody battlefield. However, it's simply that people don't understand this or don't appreciate it.

2) The strategic deterrent effect exerted by national communications media has markedly increased. People and weapons are indispensable decisive and important factors that determine which side is the victor and which side is the vanquished in a war. However, in modern societies and modern wars, information is now to some extent replacing people and weapons and permeating societies and battlefields. In modern wars, the deterrent effect of weapons exceeds in varying degrees the deterrence to be expected from the performance and power of the weapons themselves. High-tech weapons are especially noteworthy in this respect. In the war in which NATO carried out an air assault on the Yugoslav Federation, the U.S. laid out fully the nature of its high-tech weapons, using various types of communications media. The U.S. made public the performance characteristics and the manufacturing costs of its important weapons on the Internet. Its goal was not to show off its so-called "military transparency." Rather, its goal was to flaunt its wealth and its real military strength before the world, and before third world countries in particular. Some Chinese military experts have expressed very serious doubts about the publicly announced manufacturing cost of 2.1 billion dollars that the U.S. has provided for the B-2 stealth bomber. These experts maintain that this way of speaking stems primarily from the Americans' strategic goals, and that it is an attempt to "subjugate the enemy's army without fighting." [This is a reference to Sun Tzu's "The Art of War," which states: "Subjugating the enemy's army without fighting is the true pinnacle of excellence."] At the same time that the U.S. is using its national communications media for strategic deterrence purposes, it is moving heaven and earth to contain any strategic deterrent effect available to its enemies. The U.S.-fabricated "China threat theory" is this type of plot. On the one hand, the Americans do their utmost to belittle the weaponry of China's armed forces and publicize all the ways in which it is backward. On the other hand, it only need arise that China has new weaponry, and the Americans say that China is flaunting its military strength while they apply the "China threat theory." Thus, the Americans attempt to greatly reduce the strategic deterrent effect available to China--a strategic deterrent effect that we must have.

3) National communications media will alter certain principles that apply to traditional news reports. According to the traditional concept, a report must strictly abide by the principle of being faithful to the facts in order to be a genuine communications media news report. It is absolutely impermissible to create reports out of thin air and fabricate at will. Nevertheless, judging from the high-tech regional wars of the past ten years, the Western countries, and particularly the U.S., have already radically altered this concept in the process of carrying out IW via national communications media. While they take care to reveal concrete realities and advertise the so-called "truthfulness" of their news in their media communications, from an overall standpoint they operate according to their strategic needs and will in extraordinary times high-handedly fabricate reams of false information in order to achieve their goal of misleading and deceiving international public opinion. This point could not be illustrated any more clearly than it was during the war in which U.S.-led NATO bombed the Yugoslav Federation; particularly in the struggle with China for the public opinion initiative following the surprise attack on the Chinese embassy. As soon as the surprise attack incident occurred, the U.S. national communications media, before any investigation whatsoever had been carried out, flatly and categorically proclaimed it a "mistaken bombing." The non-national communications media in the U.S. also insisted virtually with one accord that it was a "mistaken bombing." According to a U.S. survey, the great weight of public opinion in the U.S., and even in the West as a whole, is in harmony with this viewpoint. Whether the results of an investigation confirm or contradict the truth and factuality of this viewpoint is already of no importance. The U.S. itself believes that it has achieved its desired goal by producing these kinds of public opinion results. Traditional communications concepts give no sanction whatsoever to intentional misleading and deception by national communications media, and traditional concepts even strongly and resolutely object to these practices. Practical experience teaches us, however, that not only does this kind of intentional misleading and deception exist, as practiced for example by the U.S. national communications media after the bombing of the Chinese embassy, but it also now plays a very important role indeed.

4) National communications media will be among the important targets in attacks that the two sides make against each other in future wars. The national communications media of the Yugoslav Federation played a major role in the Yugoslav Federation's comprehensive resistance to U.S.-led NATO both on the military battlefield and on the battlefield of the heart. Thus, when NATO deemed it necessary to carry out a major attack on the Yugoslav Federation's national communications media, it had the effrontery to openly carry out crushing bombing attacks on the Yugoslav Federation's television broadcasting system facilities, thus interrupting enemy [media] communications. In high-tech regional wars of the future, the hegemonic countries in addition to possibly carrying out this kind of "hard attack" will also perhaps make use of a number of "soft attack" measures for the purpose of damaging and/or interrupting the enemy's communications

media computer systems--soft attack measures such as: computer viruses; "worm" programs that can cause network overloads; "Trojan horse programs" that have disguised capabilities and can be activated externally; "trap doors" that have remotely controlled openings that allow for the disclosure of secrets; computer chips that have malicious instructions that can modify and change programs; and intrusions by hackers. Therefore in future wars, adequate preparations must not only be made so that national communications media can withstand "hard attacks"; measures must also be taken to guard against and counterattack against "soft attacks." As peacetime national IW is waged on an ever larger scale, the need for this latter type of preparation seems more urgent than ever.

THIS REPORT MAY CONTAIN COPYRIGHTED MATERIAL. COPYING AND DISSEMINATION IS PROHIBITED WITHOUT PERMISSION OF THE COPYRIGHT OWNERS.

Senior Colonel Huang Xing, associate research fellow at the Academy of Military Science, and Senior Colonel Zuo Quandian, research fellow of the Academy of Military Science: "'Holding the Initiative in Our Hands in Conducting Operations, Giving Full Play to Our Own Advantages To Defeat Our Enemy'--A Study of the Core Idea of the Operational Doctrine of the People's Liberation Army"

Zhongguo Junshi Kexue [China Military Science] in Chinese 20 Nov 96 No 4, pp 49-56

Document ID: FTS19970619001633
Entry Date: 06/19/1997
Version Number: 01

For operations under high-tech conditions, an important thing is to improve one's weapons and equipment. This is particularly imminent to our Army, which is still at a low level of modernization. However, in order to defeat a strong enemy, a more important thing is to change our operational doctrine, which may be the key and a short cut to our Army's victory in the future. Therefore, deepening our research in operational doctrine is an important part of our ongoing efforts to make preparations for military struggle in the new period. Many tasks have to be done before the operational doctrine can be reformed. But the most key task is to clearly define the core idea of the operational doctrine. This article will serve as a preliminary study of this question.

I. Given High-Tech Conditions, Our Army's Operational Doctrine Is About To Undergo a Profound Reform, Center of This Reform Is To Present a Core Idea of the Operational Doctrine

1. New changes in battlefield conditions due to the development of high technology are many and extensive, presenting tough challenges to our Army's conventional operational doctrine.

Local wars under high-tech conditions are the type of wars which most intensely and largely involve science and technology in human history. The extensive application of high technology has tremendously played up the role of science and technology in wars, and conspicuously changed the conditions of wars and the form of movement, which will inevitably cause changes in the guidelines, forms, and methods of operations. All such changes are particularly highlighted in the following aspects, on the battlefields of modern times.

High "visibility" on a transparent battlefield. Under high-tech conditions, all kinds of reconnaissance platforms are set up everywhere, under the water surface and in space; all means, including light, electronics, magnetism, and sound are used; all forms of reconnaissance, beyond-the-horizon, round-the-clock, all-weather, and anticamouflage, are applied to form a "broad net" for reconnaissance, monitoring, and advance warning. The coverage of a reconnaissance satellite is several 10,000 times as wide as an airplane can cover, the operational distance of a long-distance search radar can be as far as 4,800 kilometers [km], a low-light level night vision device is capable of amplifying the light level of objects during night time up to 10,000 times, and a portable thermal imaging system can detect personnel and vehicles hiding 60 meters deep in a jungle or targets buried 1 meter under the ground surface. When a flying object is flying in the air 300 meters above the ground surface, it may be monitored by 800-1600 sets of radar at the same time, and the density of the radar signal can be as high as 1.2 million pulses per second. There is no doubt that no major military operations and battlefield objects can escape from such a "net."

High-intensity, totally deep-going integrated firepower shock attack can simultaneously cover all fronts of the whole battlefield. Modern armies have many powerful means of firepower shock attack, which enable them to deliver an integrated strike ability that covers the ground, the sea, and the air at high, medium, and low altitude, reaches long, intermediate, and short ranges, and makes use of both hardware and software. As a result, to a certain extent, modern armies can be free from the restraints of such objective conditions of time, space, and weather, carry out simultaneous, all-altitude, and fully in-depth strikes on all fronts of the operational space within a fixed time span, thus they have gained an unprecedented ability to explore the space of a battlefield. For instance, the US Army can now reach a depth of 60 km in tactical attack operations, 700 km in campaign attack operations, and over 1,000 km in strategic attack operations. Integrated firepower shock attack combines deep-going shock attack with simultaneous shock attack. Its ultimate aim is to disrupt and upset the enemy's operational rhythm, undermine the enemy's operational systems at all levels, and deprive the enemy of its overall offensive and defensive capability. In the future, the integrated use by both the belligerent parties of high-intensity, totally deep-going integrated firepower shock attack will become a basic means for them to fulfill their operational purposes.

Frequent movements at a high speed result in a non-linear battlefield. In addition to shifting of armed force and firepower in the conventional sense and change in operational modes, the content of mobility has been extended. Mobility is regarded not only as a form of movement but also a major operational mode. The greatest special characteristics of mobility is its offensive nature, and its primary principle is to avoid the strong enemy while striking at the weak one. When both belligerent parties have high-speed mobility, it is necessary to emphasize the practice of increasing the speed of reaction to battlefield conditions by changing the form of the use of information, so as to ensure that one can act faster than one's enemy. It is necessary to realize the combination of mobility with firepower and shock attack at a higher level, and concentrate operational effectiveness in a decisive time and at a decisive place to attack and seize "decisive spots" and to strike at the enemy's fatal part. When our side makes a favorable move, it is necessary to pay more attention to checking and undermining the enemy's movement, prevent the enemy from enjoying freedom of movement, and so on. All these changes in the features of mobility have broken away the restrictions of a fixed battle front, make the border between the front and the rear on the battlefield ambiguous, result in the gradual disintegration of the linear echelon-type battlefield structure, thus reduce the whole battlefield into an irregular nonlinear state.

Delivering accurate strikes without real engagement make an "uncovered" battlefield possible. The increase in the battlefield transparency and long-range destructive force has tremendously increased the degree of precision and definiteness of operations. A company's reach of control can be as far as 200 km, an aircraft carrier's reach of control can be as far as 2,000 km, whereas the reach of control of a device placed in outer space can be as far as several 10,000 km. These have made a dream of many generations of servicemen--"discovering means destroying"--come true. There is hardly any unreachable part or target across the battlefield. Given the joint effects of all the above factors, a modern army is capable of dealing blows at the enemy with all kinds of indirect firepower, to the farthest distance possible, without direct engagement with the enemy.

Electronic warfare which employs both software and hardware creates an invisible battlefield. Electronic warfare has opened up the fourth dimension of battlefield, beside ground, sea, and air. Electronic warfare, which closely integrates "soft damaging," "hard destruction," and the "technology of hiding," plays a role in every aspect of modern warfare and throughout the whole process of military operations. Nowadays electromagnetic domination has become the first prerequisite for air, sea, ground, and space domination. Electronic warfare has obscured the demarcation line that marks the "beginning of engagement," and has become an intangible power on the modern battlefield. Whichever side loses in an electronic war will be reduced to "blind" and "deaf," so its weapons will be disabled, and it will lose its initiative in a battle or a campaign or even a whole strategic situation.

Integrated ground, sea, air, and space operations bring about an all-dimensional battlefield. The future battlefield will bear the special characteristics of "integrated," "joint," and "all-dimensional" operations. The powerful information network enables transmission of information about operations between different operational units at a close-to-real-time speed, the army's ability to seize and make use of opportunities for combat has been increased significantly, all operational orientations, operational fields, and the operations of all services and arms have been combined into a whole to an unprecedented extent. The operational ranges of different arms and services interweave with each other, the ground, sea, air, and space battlefields coordinate with each other, combat, supports, and logistic services are combined more closely together, thus a full, joint operation becomes possible in terms of the coordination of time, place, purposes, and resource allocation. On this type of all-dimensional battlefield, the power of joint operations by all services much outdoes the simple sum of all individual services.

Full-time and full-space command and control warfare brings about a centralized battlefield. To a very large extent, new changes in the modern battlefield are the result of new changes in the competition between the commanders of two belligerent sides and between their commanding organizations. Means of operations as products of high technology make the destruction and protection of commanding organizations more and more a focus of concern for both belligerent parties. The objective need for striking at the enemy's command and control system and for protecting one's own has naturally given rise to command and control warfare as a new operational mode. The purpose of command and control warfare is to cut off communications between the enemy's command system and its operational units. It is much easier to annihilate an enemy which loses control of its units.

The above changes in the battlefield have changed people's concepts on time, space, combat strength, battlefield structure, and operational efficiency, seriously challenging our Army's traditional operational doctrine. Therefore, updating the operational doctrine becomes an imminent task to be done in preparations for military struggle in the new period.

2. To meet the challenge, the first priority is to make a major breakthrough in the development of the operational doctrine, and the key task is to put forth a core idea for our Army's operational doctrine.

The operational doctrine is the center of the whole military theory. It serves not only as a guide to the preparations for military struggles and to future military operations, but also as an impetus to army building. Before it can meet the challenge and effect the historical switch from local war under general technological conditions to local war under modern technological, especially high-tech conditions, our Army needs to do many things. One of its major tasks is to establish a theoretical system for operations under high-tech conditions, based on the military strategic guideline for the new period. True cases of local wars after World War II have shown that under high-tech conditions, the internal relations between local wars and mechanized wars, with regard to content, structure, and form, have to a certain extent experienced substantive changes. If we fail to appropriately cope with these kind of changes, and correctly understand and handle the relations between history, reality, and the future, we will not possibly make an objective scrutiny of our Army's operational doctrine, and make it clear which part of the theory should be inherited, which part should be revised, and which part should be discarded. There are plenty of precedents of this type in history. A victorious army may often suffer from a kind of "victory syndrome," because of which they may keep an operational doctrine that proved effective in the past, and apply it to guiding future wars. The army will not realize the bad consequence of conservativeness until it finds itself unfit for the new circumstances in the next war. So, in this sense, the victory of a previous war has sown the seed of failure of the next war. This indicates how important it is to build an operational doctrine system with our Army's special characteristics to suit high-tech conditions!

The Central Military Commission has shown great concern for the research on our army's operational doctrine for high-tech conditions. All our Army, commanders and soldiers alike, have been working hard in exploring this topic and scored very good results. In the past few years in particular, the research on operational modes has become a popular trend within our Army, and many new operational modes have been developed, opening up a new chapter of the reform of our Army's operational doctrine, and laying down a solid foundation for the development of the operational doctrine system for high-tech conditions. However, if evaluated by scientific standards and by the needs of future wars, what we have achieved so far is merely an initial success, and we have yet to go a long way before any breakthrough can be made. In order to further promote the research on our Army's operational theory and to carry on the study of operational modes further in depth, first of all it is necessary to research in and put forth the core idea of our Army's operational doctrine.

The core idea of our Army's operational doctrine represents the basic understanding of our Army's operations, a very concise summary of the operational guideline, and the soul of the operational doctrine. It is a strong reflection of the dialectic relations embodied in operation guidance, and the idea of giving full play to our Army's strong points to fulfill the goal of "the weak defeating the strong." It serves as an important orientation in defining and regulating our Army's operational guideline and principles, and its basic operational modes as well. Based on this understanding, we may say that putting forth the core idea of the operational doctrine is of crucial significance to the further exploration and updating of our Army's operational doctrine.

II. The Core Idea of Our Army's Operational Doctrine for High-Tech Conditions Should Be: 'Holding the Initiative in Our Hands in Conducting Operations, Giving Full Play to Our Advantages To Defeat Our Enemy,' Which Is the Outcome of the Combination of Our Army's Traditions, Experiences With Modern Conditions

1. "Holding the initiative in our hands in conducting operations, giving full play to our advantages to defeat our enemy" is the core idea of our Army's operational theory for high-tech conditions.

The idea of "holding the initiative in our hands in conducting operations, giving full play to our advantages to defeat our enemy" is not a guideline or principle governing operations, still less a specific mode of operation, but rather an idea which dominates the operational guideline, principles, and mode, and which thoroughly permeates into the whole operational doctrine. It is the highest standard our Army is pursuing of operations under high-tech conditions. Its basic spirit can be summed up into the following points:

First, it is necessary to emphasize the necessity of not being scared by any powerful enemy but building up our confidence in victory. This is a very important point, and the basis of the principle of "holding the initiative in our hands in conducting operations, giving full play to our advantages to defeat our enemy." Our Army's war experience has proved that the very first thing for any operation under any circumstances in any time is that we must not be terrified by any powerful enemy, and influenced by an enemy who is temporarily holding the initiative, instead we must be fully aware of our strong points and the favorable conditions we are enjoying, and we should firmly believe that we can reverse the balance of power between us and the enemy, thus defeating the enemy at last. To seize the initiative on the battlefield, we must first of all keep the initiative in operation guidance or operation planning; otherwise we will be mentally captured by the enemy, and will be bound to lose. Without holding to this ideological preconditions, our victory in operations will be impossible, and a correct operational doctrine will be out of the question.

Second, it is necessary to lay stress on gaining the initiative in our own hands, and never should we be led by our enemy in conducting operations. Gaining the initiative in our own hands does not mean dominating an operation, instead it is a precondition for domination of the operation. Gaining the initiative in operations mainly means that the unit providing guidance in operations is to keep the initiative in its own hands, in other words, when the commanding body is pondering on operational issues, it must always uphold the principle of "proceeding in everything from one's own needs"--striking at whatever targets promise the best results; striking out whenever and wherever it is most suitable; and fighting the battle in whichever form and by whichever means is necessary to win the easiest victory possible. In other words, we should not fight with the enemy in a way anticipated by the enemy, in a time and in a place that the enemy are expecting. Only in this way, will we be able to change inferiority into superiority, and passiveness into activeness, and thus win the initiative in conducting operations.

Third, it is necessary to lay stress on giving full play to our own advantages and on utilizing our strong points to attack the enemy's weak points. Strong and weak points are defined in a relative sense, and they may change as time goes by. Every army has its own strong and weak points. Strong and weak points exist in any time and under any circumstances. The principle of "holding the initiative in our hands in conducting operations, giving full play to our advantages to defeat our enemy" means to comprehensively and dialectically see both the enemy's strong and weak points and ours as well, correctly giving full play to our own strong points and avoiding the enemy's strong points in conducting operations, and striking at the enemy's weak points and shielding our own weak points. This is the most basic idea and approach to change the balance of combat effectiveness and to reverse the situation on the battlefield. Utilizing our strong points to attack the enemy's weak points seems to be a simple thing to do, but actually it is not. The crux to the problem is that: when evaluating the enemy's and our own strong and weak points, we must do away with hidebound thinking, and make specific analysis of specific cases in light of local and current conditions and in accordance with our operational targets, thus finding out the enemy's and our own specific strong and weak points in each specific operation. In utilizing our strong points to attack the enemy's weak points, we must display courage in taking reasonable risk, dispel misgivings, and be adept at doing away with all negative factors. As soon as we can find out and focus our attention on our major strong points and the enemy's major weak points, we will be able to readily make up our minds and take resolute actions.

[passage omitted]

3. The idea of "holding the initiative in our hands in conducting operations, giving full play to our advantages to defeat our enemy" can serve as a clear guideline for the development of our Army's operational doctrine.

The idea of "holding the initiative in our hands in conducting operations, giving full play to our advantages to defeat our enemy" is put forth for the following purposes:

First, it helps further unify the doctrine for operational guidance for the whole Army. At present, our Army has a clearly defined strategic guideline and, generally speaking, we are following a unified doctrine for operational guidance. However, since the military strategic guideline for the new period was implemented only lately, our Army is still undergoing the "two transformations" regarding preparations for military struggle and army building, and we are still seeking solutions to many problems, it seems that we have to wait for a while before a complete consensus can be reached on the operational doctrine. For example, whenever talking about our existing weapons and equipment, some people would always say they are obsolete, and they just have no confidence in our Army's ability of winning local wars under high-tech conditions with the existing weapons and equipment. Some people have gotten used to thinking according to foreign ideas on operations and army building, but refuse to thoroughly study our Army's heritage and experience and the up-to-date situation of our Army and the enemy. In pursuit of the so-called advanced trend and high or super standards, they are just blindly following behind others. The causes of these problems are manifold. Undoubtedly one of the major causes is the lack of a very expressly defined, dominant idea guiding the reform of the operational doctrine. The adoption of the idea of "holding the initiative in our hands in conducting operations, giving full play to our advantages to defeat our enemy" can help clarify some muddy concepts and further unify our thinking on operational doctrine.

Second, it helps establish our Army's operational theory system for high-tech conditions. For quite a long time in the past, our Army's operational doctrine was to mainly cope with "deep-going and high-speed offensives on a long front," with the focus placed on how to "fight with tanks, aircraft, and airborne forces." As our major operational objects have changed, major changes have taken place in the direction of the study on the military traditions, military strategy, and operational ideas of the enemy in whom we are interested. These changes will make direct, far-reaching impacts on our Army's study of future operations. When observing our new rivals, how can we free ourselves from both explicit and implicit influence of old conventions, familiar rules, and outdated concepts, and how can we ensure that the actual circumstances are taken into consideration? This problem has yet to be solved. The adoption of the guideline of "holding the initiative in our hands in conducting operations, giving full play to our advantages to defeat our enemy" can help us get a clear picture of our operational objects' and our Army's situation. By following this idea throughout the study of operational doctrine, we can develop a basic understanding of our Army's operations under high-tech conditions, and with this idea as its backbone, we will thus be able to make a breakthrough in our research on operational doctrine.

Third, it helps deepen our Army's study of operation modes. The core idea of our Army's operational doctrine for high-tech conditions needs to be supported by a guiding ideology, operational principles, operational forms, and a complete set of effective operational modes, all to suit high-tech conditions. The role of this core idea in guiding the study of operational modes is mainly reflected in that it not only retains the special characteristics of our Army's operational modes but also suits the real needs of operations under high-tech conditions. Centering around our Army's needs, we are to dialectically integrate history, reality, and the future. Otherwise, we may get lost in our study of operational modes; and the operational modes finally developed by us will either fail to reflect the special characteristics of our time, or will be too advanced to suit our Army's actual conditions. The adoption of the idea of "holding the initiative in our hands in conducting operations, giving full play to our advantages to defeat our enemy" can help us further activate our thinking in the study of operational modes. It provides an orientation and a test reference for the development of a complete set of operational modes for high-tech conditions, which will represents the integration of our Army's traditions and experience with modern conditions.

III. Rich in Content, Idea of 'Holding the Initiative in Our Hands in Conducting Operations, Giving Full Play to Our Advantages To Defeat Our Enemy' Means in Substance To Gain Greater Initiative in Operations

The idea of "holding the initiative in our hands in conducting operations, giving full play to our advantages to defeat our enemy" is rich in content. The whole idea can be summed up into seven points, all of which point to an essential objective--to gain greater initiative in operations.

1. Importance is attached to both the role of technology and the application of strategy.

Some people classified the styles of the art of war into two major types according to the differences between the East and the West in military traditions and culture. They said: "The West places stress on technology, while the East on strategy." Although this description may not be very accurate, it summarizes to a certain extent the different styles of Eastern and Western arts of war. Western countries have made rapid progress in science and technology in the modern and contemporary times. They enjoy an obvious scientific and technological superiority in wars. In order to win a victory in their wars for national liberation or war against aggression, some developing Eastern countries naturally have to count on their traditional superiority in the use of strategy for making up their technological weakness. This indicates that the use of strategy can reverse the balance of combat strength due to the varying technological standards of weapons and equipment. However, strategy and technology are a pair of opposites which form a unity. While restraining the role of technology, the use of strategy can also give a greater play to technology. The perfect integration of strategy and technology will result in the most ideal performance of operational guidance. In operations under high-tech conditions, our Army's weapons and equipment may be much inferior to that of our strong enemy. In order to defeat our enemy, not only must we improve our weapons and equipment as soon as possible and allow full play to weapons and equipment, but we must also give a greater play to our initiative in operational guidance, competing with the enemy by using wits, strategies, and especially new, original ideas in the integration of high technology and strategies, and exploring new frontiers and scaling new heights in operational guidance. This is the very basic point of the idea of "holding the initiative in our hands in conducting operations, giving full play to our advantages to defeat our enemy." In this connection, on the one hand we must sum up our Army's experience in the combined use of technology and strategy in past operations; on the other, we must attach great importance to the research on the integration of the use of strategy with our Army's existing weapons and equipment, especially those high-tech weapons and equipment that have been scheduled to be put into commission, with a view to updating our Army's modes of operation.

[passage omitted]

4. It is necessary to break the bounds of different services and arms and organize operational forces according to the type of missions.

Under high-tech conditions, our Army must give full play to the integrated power of joint operations, attach great importance to the strategy of cultivating a program by combining different nodes on the battlefield, accomplish an optimal combination of all operational forces, form joint operation systems to carry out different missions, and efficiently combine the combat effectiveness of different services and arms so that the armed forces, in different structural forms, can exercise their functions to the most optimal extent. In the past, our Army used to organize its operational forces by different services. So forces of a same nature which were supposed to carry out the same sort of mission were designated to different services. This tremendously hindered the efficient combination of operational forces. Given the fact that our Army has only a limited number of high-tech operational units, it is still harder for this old organizational form to meet the needs of operations under high-tech conditions. According to the ideas of "holding the initiative in our hands in conducting operations, giving full play to our advantages to defeat our enemy," we must update our concepts, break the bounds of different services and arms, group together all the operational forces of different services and arms that have the same nature and are supposed to carry out the same sort of missions, and reorganize them in a centralized manner according to the needs of operations. We must view and distinguish the different natures of different forces in a new perspective, and group reconnaissance and electronic countermeasure units together as operational units for operations under high-tech conditions. By the same token, we may reorganize our operational forces roughly into a few systems, including the joint reconnaissance system, the joint electronic countermeasure system, the air joint-attack system, the naval joint-attack system, the ground joint-attack system, and the joint-logistic service system.

[passage omitted]

6. It is necessary to focus on destroying the enemy's operational system and structure, and to place stress on the tactics of striking at the enemy's weak parts to cause a drastic decrease in its overall combat strength

Modern warfare is a rivalry between systems. Given the trend that operational forces are more and more heavily relying on information networks and systems which help bind them together to form an integral whole, certain "nodes" in the operational structure, which serve as the key components enabling the system to exercise its operational functions, are in fact the fatal parts of the system most vulnerable to attack and destruction. It is obvious that an army can more easily dominate the war situation by paralyzing its enemy than by annihilating part of the enemy's forces. Therefore, in operations under high-tech conditions, we must not only focus on annihilating the enemy's combat effectiveness, but must, first of all, pay attention to and place stress on striking at "nodes" of the enemy's operational system, so as to destroy and paralyze the enemy's operational structure. With regard to operational guidance, we must try our best to find out in good time the structural weaknesses of the enemy's operational system, including the essential weak links of the enemy's whole national infrastructure which supports the enemy's operations; then we can use precision guided weapons, deep-striking forces, and special operational forces to swiftly bypass the enemy's strong nodes, skillfully direct our firepower to the enemy's weak links, and give it a fatal strike. In the meantime, we must always be prepared for anti-structural-destruction strike back from the enemy, make sure our fatal parts are well protected, and keep our operational system in stable conditions. The idea on destroying the enemy's operational system and structure represents the development trend of modern offensive and defensive operations. To a weaker army in a war, this idea will even provide a "leverage" mechanism. This is exactly the crux of the principle of "holding the initiative in our hands in conducting operations, giving full play to our advantages to defeat our enemy."

7. It is necessary to exercise centralized, unified command and independent, resolute decisionmaking at a higher level, in light of the actual situation on the battlefield. Operational command is a core issue of operation. Under high-tech conditions, operational command has undergone a series of profound changes, of which the most spectacular are: (1) the development of information technology, which has enabled for the first time the close-to-real-time transmission and sharing of intelligence and information, and led to a reduction in commanding levels; (2) the introduction of the command automation system, which has tremendously shortened the process of reconnaissance and judgment, decisionmaking, and execution, and which significantly enhanced command efficiency; and (3) extraordinarily intense warfare of command and control, which has made the role of command more prominent, presented an unprecedentedly serious threat to the survival of the command system, thus bringing up the maintaining of a stable command as a serious problem. To get adapted to these changes, we must solve the problem concerning commanding means, and still more must we solve the problem concerning our concepts on command. After the Gulf war, people have focused their attention most on such problems as how to increase the total amount of intelligence, information, and operational instructions, how to increase the transmission speed, and how to further strengthen the automation system. To be sure, it is right to keep abreast with this development trend. Nevertheless, confining one's attention to these changes alone but ignoring the most essential aspects of operational command can usually be misleading. No matter how technological conditions are evolving, the basic problem that needs to be solved regarding operational command will remain the same-how to ensure that subjective guidance suits the actual conditions on the battlefield. Here the key lies in the commander's initiative. This is the reflection in the field of operational command of the spirit of "holding the initiative in our hands in conducting operations, giving full play to our advantages to defeat our enemy." As far as the use of the form of command is concerned, to give full play to the commander's initiative means to achieve at a higher level the integration of a centralized, unified command and independent, resolute decisionmaking, with the former dominating the latter, but with no undue stress on either aspect. We have always attached importance to centralized command. Now the point that merits attention is, how we are going to give full play to the initiative of commanders at lower levels, and encourage them to boldly and skillfully use their discretion and to act resolutely and independently, in light of the changing conditions on the battlefield, guided by the general operation intention. During an operation, especially after a decision is made, in order to prevent communication between our commanding organization and its subordinate units from being cut off by the enemy, which may cause decontrol of and disorder in the operation, our Army should make every effort to reduce the total amount of communications between the superior and subordinate units, and to confine battlefield information exchange mainly to transmission of crucial intelligence and instructions or of those about the overall operation conditions. As viewed from the principle of integration of centralized, unified command and resolute, independent decisionmaking, the ideal state of operational command that we are looking for can be described as follows: all the operational forces of our Army, from the leadership down to grassroots units, can independently carry out operations, giving full play to their initiative, making use of their strong points, and striking at the enemy's weak points, without over-relying on smooth communications.

The above elaboration on the idea of "holding the initiative in our hands in conducting operations, giving full play to our advantages to defeat our enemy" is merely the authors' immature thinking on the core idea of our Army's operational doctrine. Our purpose in presenting our views is to find out the very essence of the operational doctrine, and use it as a general guidance in our study of the operational doctrine. We hope our attempt will contribute to the reform of our Army's operational doctrine.

THIS REPORT MAY CONTAIN COPYRIGHTED MATERIAL. COPYING AND DISSEMINATION IS PROHIBITED WITHOUT PERMISSION OF THE COPYRIGHT OWNERS.

[This page is intentionally left blank.]