Monographs

11-1-2001

Chinese Information Warfare: A Phantom Menace or Emerging Threat?

Toshi Yoshihara Mr.

Follow this and additional works at: https://press.armywarcollege.edu/monographs

CHINESE INFORMATION WARFARE:
A PHANTOM MENACE OR EMERGING THREAT?

Toshi Yoshihara

November 2001

FOREWORD

Mao Tse-tung counseled, "To achieve victory we must as far as possible make the enemy blind and deaf by sealing his eyes and ears, and drive his commanders to distraction by creating confusion in their minds." Few concepts mesh so contextually with Mao than the Chinese approach to Information Warfare (IW). As the People's Republic of China struggles with its national military strategy, IW offers opportunities to win wars without the traditional clash of arms.

In this monograph, Mr. Toshi Yoshihara explores what he perceives to be China's pursuit of IW as a method of fighting asymmetric warfare against the United States. Largely imitative of U.S. thoughts, literature, and practices on IW, he believes the Chinese are seeking ways to adapt it to their own style of warfare. Paradoxically, he observes that the Chinese have not gleaned their intelligence through espionage, but through careful scrutiny of U.S. IW in practice. The Persian Gulf War and Kosovo conflict have provided ample largess to the Chinese archives.

Mr. Yoshihara examines those aspects of IW—PSYOPS, Denial, and Deception—that China believes provides the greatest prospects for victory in a conflict. Not surprisingly, Sun Tzu is interwoven into this emerging theory. Targeting the enemy's "nervous system" at all levels, that is, his ability to gather and assess information and then transmit orders, provides significant advantages in the prosecution of a campaign. Targeting the enemy's homeland defenses and its citizens can potentially end a war before it even starts. He concludes that the extent of Chinese advances or intent regarding IW is difficult to ascertain given its closed society. Chinese IW may still be nascent, but the menacing intent is there and only vigilance will protect the United States.

Much in the realm of IW remains speculative and conceptual. Aspiring nations can take advantage of the Revolution in Military Affairs by skipping generations of technology and becoming a modern, sophisticated threat, obviating the need for significant financial investments. The consequences of the threat are of great import to today's strategic leaders and thinkers. The Strategic Studies Institute is pleased to offer this monograph as a topic of debate that will continue into the millennium.

DOUGLAS C. LOVELACE, JR.
Director
Strategic Studies Institute

BIOGRAPHICAL SKETCH OF THE AUTHOR

TOSHI YOSHIHARA is a Research Fellow and the resident expert on security issues in the Asia-Pacific region at the Institute for Foreign Policy Analysis. His research areas at the Institute include American alliances in the Asia-Pacific, China's military modernization, China-Taiwan relations, Japan's security policy, critical infrastructure protection, and energy security in the Persian Gulf. Mr. Yoshihara was an analyst focusing on China's security policy and military modernization at the RAND Corporation and the American Enterprise Institute. He was a Visiting Fellow at the Fletcher School of Law and Diplomacy, Tufts University (1998-2000). Mr. Yoshihara received a B.S. in International Affairs from Georgetown University's School of Foreign Service and an M.A. in International Affairs from Johns Hopkins University's School of Advanced International Studies (SAIS). He is currently a doctoral candidate at the Fletcher School of Law and Diplomacy, Tufts University, working on his dissertation on Chinese military innovation and information warfare.

SUMMARY

In recent years, China has demonstrated an intense fascination with information warfare (IW). The potential advances in Chinese IW doctrine and capabilities have direct implications for U.S. national security. The ability of China to conduct information warfare against the United States in peacetime, confrontation, or conflict could pose severe challenges to defense planners. Yet, American understanding of China's approaches to IW within the academic and defense communities remain shallow. This lack of understanding, both stemming from the extreme secrecy surrounding China's military programs in general and the nascent stage of development in IW in particular, could invite ugly strategic and operational surprises for the United States.

As an initial step to clarify the future direction of Chinese IW and to identify new areas for further research, this monograph explores Chinese perspectives of information warfare through a sampling of the burgeoning open literature circulating in China. The monograph provides a preliminary assessment of these Chinese writings and analysis. It demonstrates some linkages and parallels to America's current debates on IW, the Soviet-U.S. competition, Clausewitz's classic dictums, and Chinese strategic culture. The monograph concludes with implications of future developments in Chinese IW for American policy.

CHINESE INFORMATION WARFARE A PHANTOM MENACE OR EMERGING THREAT?

Dazzled by Information Warfare.

In the past decade, China's military modernization and growing interest in the revolution in military affairs (RMA) have increasingly attracted international attention. Like many other military powers, China has exploited the unprecedented general peace in the international security environment to reexamine and experiment with its own defense capabilities and doctrine. In particular, the concept of information warfare (IW) has emerged as a subject of great interest in Chinese military discourse. The intense discussions and debates within China's defense community suggest that Beijing may be harnessing the political will to devote substantial resources to developing IW doctrines and capabilities. China's potential ability to leverage the information revolution accompanied by its gradual rise as a major military power have led many observers to speculate whether China might succeed in becoming one of the global leaders in IW.

China's appreciation for the centrality of information as a tool of statecraft and military power has significant implications. Given the tremendous advances in information technologies both in terms of the rate of innovation and quality of improvements, China is well positioned to exploit this revolution. Just as China has surprised skeptical observers with its rapid developments in nuclear weapons, ballistic missiles, and space programs, the Chinese may similarly come to the forefront in IW. More importantly, China's focus on IW presents a potentially daunting challenge for American defense planners. In two cyber-attack exercises in 1997 and 1999, the U.S. military found that a group of hackers "using publicly available

resources was able to prevent the United States from waging war effectively." The Pentagon premised the first drill on a military crisis on the Korean Peninsula. The result of the exercise was sobering: the series of attacks against civilian and military networks had a paralyzing effect on American command and control at the highest levels of leadership. It is therefore conceivable that IW could provide China with the capacity to hinder American military operations in the Asia-Pacific, a region of central importance to U.S. national security interests. Hence, the direction of China's IW strategy has direct policy relevance to the United States.

In recent years, the Chinese have demonstrated a voracious appetite for examining IW. Arguably, only the United States and Russia rival China's analytical work in IW. The exotic concepts and capabilities of IW have seemingly captivated the imagination of Chinese futurists and military strategists alike. Indeed, a virtual cottage industry has developed around the topic in Chinese literature on military affairs. How China will translate theoretical discussions on IW into practice will be an increasingly important policy question for the United States.

The author first explores Chinese thinking on IW through a literature survey of primary sources. Strategists have demonstrated a keen interest in understanding the theoretical concepts, requirements, and capabilities necessary to conduct IW in future conflict. The second component of the monograph assesses the existing Chinese IW literature. While Chinese thinkers have clearly begun to grapple with the opportunities and challenges of waging IW, the analytical gaps in their writings suggest that China still has a long way to go before it can embark on the quest for information supremacy (if that is, in fact, Beijing's goal). Finally, the author speculates on how Chinese thinking on IW could impact its future application. While the evidence remains scant at present, how the Chinese might use IW to achieve their political objectives may have unsettling

consequences for the United States. This monograph is not a call to arms for American defense planners. However, the potential path that China might pursue in IW and the associated risks to U.S. national interests warrant careful observation and preparation against surprise.

What is IW?

Since the concept of IW emerged in the mid-1990s as a topic of heated debate, its definition remains in a state of continual flux. Scholars, think tanks, and the U.S. Government have all struggled to provide an intellectual construct for the study of IW. Efforts to grapple with this "exotic" type of warfare continue today, and little consensus has yet emerged. The intellectual fever to come to grips with IW has also spread to China, resulting in similar degrees of disagreement over the meaning of IW. The conceptualization of IW in the Chinese context has been even more confused given that Beijing, by the nature of its opaqueness, has not published any official documentation of IW as a guide for national policy. There is no discernible taxonomy that can be meaningfully used to accurately depict Chinese IW. Only China's open sources, many of which are of dubious quality or reliability, have offered some clues on Chinese thinking.

While not an exact scientific measure, a sampling of U.S. doctrinal writings on IW could provide a useful frame of reference and possibly some context for comparison between Chinese and American thinking. According to a document on U.S. joint doctrine entitled *Information Operations*, IW is "actions taken to affect an adversary's information and information systems while defending one's own information and information systems." The Pentagon's *Joint Vision 2020* adds that, "Information operations also include actions taken in a noncombat or ambiguous situation to protect one's own information and information systems as well as those taken to influence target

information and information systems."[3] These vague definitions of IW clearly require further clarification.

At the heart of IW is information. Information guides decisionmaking in peacetime and war at the strategic (a decision to declare war), operational (a decision to move a division of forces forward for an attack), or tactical (a decision to order an aircraft to engage) levels. These decisions in turn trigger action. The purpose of IW is to affect the adversary's decisionmaking process and associated actions to one's own advantage. The outcome for the enemy can be wrong decisions, late decisions, or no decisions at all. This enables the attacker to control the opponent or, failing that, to prevent the adversary from carrying out a decision. To succeed in IW, one must achieve information superiority over the enemy. *Joint Vision 2010* defined information superiority as "the capability to collect, process, and disseminate an uninterrupted flow of information, while exploiting or denying an adversary's ability to do the same."[4] Information superiority requires both offensive and defensive components. In Joint Vision 2020, information superiority is simply understood as an "imbalance in one's favor in the information domain."[5]

There are six central pillars of IW in the current American lexicon:[6]

• *Physical Attack/Destruction*: The use of kinetic force, such as cruise missiles, to inflict damage on enemy systems or personnel sufficient to render them unusable. This type of IW can be used defensively to prevent the adversary from using offensive IW.

• *Electronic Warfare (EW)*: The control of the electromagnetic spectrum to undermine the enemy's electronic warfare capabilities through electromagnetic energy, directed energy, and antiradiation weapons.

• *Computer Network Attack (CNA)*: The use of computers and telecommunications equipment to disrupt,

deny, degrade, and destroy enemy computers, computer networks, and the information being transmitted.

• *Military Deception*: The manipulation, distortion, and falsification of information to mislead or deceive the adversary's military commander, thereby forcing the enemy to act (or not act) to its own disadvantage.

• *Psychological Operations (PSYOPS)*: The use of communications (such as propaganda) and actions intended to mislead to influence the perceptions, motives, and emotions of the enemy.

• *Operations Security (OPSEC)*: Security measures that prevent the enemy from collecting or analyzing information that may be useful to it.

A recent study uses U.S. joint doctrine as a construct to highlight the differences between Chinese and American IW. Kate Farris argues that, "the U.S. tends to focus on the CNA aspect of IW, while the Chinese take a more broad perspective, emphasizing pillars such as PSYOP, Denial, and Deception."[7] While the author's selection of Chinese literature persuasively supports this assessment, the current state of Chinese IW is simply too immature and not well enough understood to reach any definitive conclusion. As Farris herself admits, "the Chinese debate on IW is still evolving, there is some uncertainty remaining over how they will incorporate IW into their military doctrine and strategy."[8] Clearly, more data and continued observation of Chinese developments are required. Her analysis nevertheless highlights the potential utility of comparative analysis for better understanding Chinese thinking on IW. Indeed, subsequent sections of this monograph show how closely Chinese interpretations dovetail with (if not copy) America's ongoing examination of IW.

Triumph of the Information Revolution?

What explains China's intense interest in IW? At the broadest level, the Chinese clearly realize the implications

5

of the information revolution. First, China recognizes the importance of high technology and the growing power of information in the era of globalization and interdependence. Second, China aspires to become a major political and economic player in a global community where information power retains a critical place in dictating interstate relations. Given that economic development remains its highest national priority, China's integration into the information-based international economic system has in turn magnified the appeal of information. Third, as a corollary to the previous point, the Chinese believe that, as China increases its comprehensive national power, the world will eventually shift from a unipolar to a multipolar world, in which the People's Republic of China (PRC) will be a coequal.[9] In sum, the ability to compete economically and wage high-technology warfare with information technologies will be critical components of China's national strength.

From a strategic and military perspective, IW promises to compensate for China's largely antiquated conventional armed forces. First, IW could enable the Chinese to fight from a position of relative weakness, particularly against far superior military powers like the United States and Japan. In recent defense parlance, information technologies provide "asymmetric capabilities" to state and nonstate actors. While definitions of asymmetric warfare have varied and evolved over time, the basic concept is the use of unorthodox methods and capabilities that avoid or undercut an adversary's strengths while inflicting disproportionate damage on the enemy's weaknesses.[10] In a hypothetical confrontation between China and the United States, the backwardness of Chinese forces would undoubtedly invite defeat. Since the Chinese cannot possibly hope to fight on American terms, they must therefore find other means to deter or defeat the United States. IW provides Beijing with the potential capacity to reach directly into the American homeland, which has been far beyond the very limited power projection capabilities of China's military. The

6

Chinese could attack vulnerable critical infrastructures in the United States to influence or manipulate domestic public perceptions and, in turn, weaken America's political will to intervene or fight. This need to leverage weakness in order to defeat a superior foe, a central and still influential philosophy of Mao Zedong's people's war concept, has a powerful hold on Chinese thinkers.

Second, many Chinese believe that IW is one of the few technological arenas where the contest for supremacy among the great powers remains undetermined. By exploiting the information revolution, China hopes to leapfrog generations of obsolescent technologies in order to catch up with the developed world.[11] The Chinese believe that IW could offer a low-cost, quick fix to their backward forces, especially when compared to a full-fledged military build-up. America's conventional military supremacy, a critical benchmark for the Chinese military, further underscores the difficulties of overcoming conventional military inferiority. Chinese strategists hope to capitalize on the integrative powers of information technologies to improve the performance of existing equipment without incurring prohibitive expenses.[12] A prominent phenomenon in the information technology revolution (popularly known as "Moore's Law") is that, while information processing power has accelerated over the last 2 decades, the costs per unit capacity have plummeted at an exponential rate.[13]

However, this proposition holds true only for specific items and capabilities. The costs of systems or architectures that support the warfighting end of the military force have actually risen significantly relative to conventional military items. As Martin van Creveld points out, "even as the per-bit cost of data processing fell by a factor of ten over each of the three decades from 1950 to 1980, the cost of command systems rose so much that it now threatens to swallow up entire defense budgets."[14] He presciently concludes, "Given the problem of rising costs, the dilemma is likely to become even more important in the future."[15] Similarly, the pace of Chinese development in IW will largely "hinge on" the costs

of IW capabilities that Beijing hopes to exploit. Depending on how broadly the Chinese conceptualize IW and which aspect(s) they want to pursue, some items or systems may be beyond China's reach at present. For example, information-gathering tools, such as reconnaissance satellites and the associated support systems, require substantial and sustained financial commitments. Beijing has not tangibly demonstrated the political will to embark on such an ambitious modernization effort. While China's economic growth has been spectacular in the past 2 decades, stagnant trends in recent years have already defied the euphoric linear projections of some economists. Hence, IW as an alternative to conventional military power may not be sustainable or realistic in the long term. Nevertheless, this line of reasoning on the benefits of information technologies has remained compelling for Chinese military thinkers. China has therefore not discounted itself from this technological race.

Third, the Gulf War highlighted the growing centrality of IW. The high-tech weaponry (supported by sophisticated information systems) showcased during the conflict and the wholesale destruction of advanced weapons (largely Russian and Chinese in origin) shocked and galvanized the military leadership. Similar to America's "Vietnam Syndrome," China was just emerging from the deep malaise in the aftermath of the bloody and inconclusive war against Vietnam in 1979. The apparent inferiority, perhaps even irrelevance of Chinese equipment compared to American weaponry during the Gulf War finally spurred the People's Liberation Army (PLA) to embrace the study of high-technology war and, particularly, IW. In 1993, General Liu Huaqing, the former Vice Chairman of the Central Military Commission and the vocal military leader credited with starting China's current military modernization, lamented the failure of the PLA to meet the standards of modern warfare. He pointed specifically to the Gulf War conflict as the model for the Chinese when studying future

wars.[16] Chinese interest in this area intensified further in the aftermath of the NATO air campaign over Kosovo.[17]

The appreciation for information and its potential advantages in future warfare led Chinese analysts to speculate and theorize on how they might acquire their own set of doctrine and capabilities. Subsequent writings since the mid-1990s have demonstrated a keen interest (though not necessarily the analytical capacity) among strategists to explore, study, and absorb IW. Similar to the vague descriptions of IW currently circulating in America's defense community, China's evolving and fluid debates on IW have thus far remained abstract. At present no clear consensus has yet emerged in China on the specific aspects of IW the Chinese hope to develop. As a latecomer to the realm of IW, China has little foundation on which to base its intellectual discourse. As a result, the Chinese have often mimicked unclassified American works and security debates on IW as the literature survey below illustrates. More interestingly, many have tried to express their views by applying or comparing Sun Tzu's *Art of War* to IW. These efforts to adopt IW by finding new expression in strategic tradition could have profound influences on how the Chinese approach IW. The intersection between Beijing's own conception of IW, which is still in the embryonic stages, and China's strategic culture may produce strategies that are uniquely Chinese. The resulting degree of divergence from Western understanding of IW could enable China to harness the potential for unleashing ugly surprises against its adversaries.

The Chinese Buy into the RMA.

China's analysis of the RMA was the central starting point for recent Chinese discussions on IW in the 1990s and the early 21st century. Chinese military strategists have devoted significant energy in the study of the RMA for more than a decade. For example, analysts monitored closely Soviet Marshall Nikolai Ogarkov's work on America's

revolution in technical military affairs in the 1980s. However, the notion of an RMA did not gain genuine currency in Chinese military circles until after the Gulf War. The Kosovo air campaign further reinforced the growing awareness of IW.

As a result of these two major high-technology conflicts waged in the past decade, Chinese military analysts generally recognize and accept that some type of revolution in warfare is afoot. One strategist noted that the command and control capabilities demonstrated during Desert Storm represented a "great transformation."[18] One article marveled at the perfect execution of the conflict. Another writer declared, "The unfolding of the new military revolution worldwide is a prominent feature of the international security situation . . . [It] involves such fields as military thinking, military strategy, operational doctrine, military organization, and arms development."[19] One analyst further elaborated on this new military revolution stating that, ". . . there will be an overall qualitative leap in the military field of all countries—the possession by the military forces of high-quality personnel, integrated C4I systems, high-level training and education, intelligent arms, scientific organization, and creative military doctrines."[20] A Chinese commentator made an even more sweeping claim that "the beginning of the 1990s opened the curtain on the information war era and marked the sudden appearance of the third military revolution."[21]

As the last observation hinted, the Chinese recognize that information technologies are an integral part of the so-called RMA. Chinese strategists clearly identify the direct link between information superiority and victory in conflict. One article noted that the information technology revolution is the

> core and foundation of this military revolution, because information and knowledge have changed the previous practice of measuring military strength by simply counting the number of armored divisions, air force wings, and aircraft carrier battle

10

groups. Nowadays, one must take into account some invisible forces, such as computing capabilities, communications capacity, and system reliability. [22]

According to another analyst, "Information technology has . . . become an indispensable means for better command and communication. Combat between opposing forces is, firstly, between their capabilities in gathering, processing, and analyzing information."[23] The author argues that the ability to decide and act faster and better than the enemy—a central concept of American information superiority—is a prominent part of modern conflict. In future wars, weapons systems and military units will be increasingly "information-intensified."[24]

These statements on the characteristics of the RMA demonstrate a strong conviction among some Chinese military analysts that information technologies will be the critical foundation for success in future wars. Recent Chinese literature on IW also suggests that strategists have gradually developed a deeper understanding of IW. Indeed, some general conclusions on the future of IW may be coalescing among Chinese analysts.

Chinese Views on IW Strategies.

Major General Wang Pufeng, widely recognized as the founder of Chinese IW, produced a sweeping working definition of IW. According to the author:

> Information war is a product of the information age which to a great extent utilizes information technology and information ordnance in battle. It constitutes a "networkization" (*wangluohua*)of the battlefield, and a new model for a complete contest of time and space. At its center is the fight to control the information battlefield, and thereby to influence or decide victory or defeat.[25]

Another definition synthesizes a more concrete Chinese understanding of IW:

11

IW is combat operations in a high-tech battlefield environment in which both sides use information- technology means, equipment, or systems in a rivalry over the power to obtain, control, and use information. IW is a combat aimed at seizing the battlefield initiative; with digitized units as its essential combat force; the seizure, the control, and use of information as its main substance, and all sorts of information weaponry [smart weapons] and systems as its major means.[26]

More specifically, the main objective of information war is to attack the adversary's information systems while protecting the information infrastructure of one's own forces. Based on a large collection of Chinese primary sources, James Mulvenon argues that, "the aim of IW in the Chinese literature is information dominance [*zhixinxiquan*]."[27] Similar to the American concept of "information superiority,"[28] Chinese IW seeks to disrupt the enemy's decisionmaking process by interfering with the adversary's ability to obtain, process, transmit, and use information. The paralysis of the opponent's information system and decisionmaking cycle would, in turn, destroy the adversary's will to resist or fight on. For instance, IW would attack the enemy's command and control systems in order to confuse or blind enemy forces. This notion of attacking the adversary's command and control systems mirrors the strategies employed during the Gulf War and the Kosovo air campaign. In both conflicts, American forces launched an intensive effort to destroy and bring down the enemy's "nervous system" in order to weaken the ability of the enemy's kinetic weapons force to respond or fight. However, Chinese discussions broaden IW further. Some analysts argue that an effective information attack could completely disrupt an adversary's military operations and therefore preclude the need for a direct military confrontation. The author examines at length whether the Chinese have mistakenly lost sight of the need to field a kinetic weapons force in tandem with command and control warfare.

This IW concept of attacking and destroying the enemy's command and control capabilities has received great

attention among Chinese commentators. One analyst argues that IW combat is a struggle between the command and control systems of the opposing forces. He asserts, "A winning force enters the battle after already winning the battle . . . The goal that confrontation of command pursues is to 'win in strategy,' because only by doing so can one win a war or even stop a war."[29] In other words, the side that wins in the struggle for battlefield command determines the outcome of wars. He observes that the multinational forces in the Gulf War defeated Iraq by first destroying its ability to command its forces. "Without the power to 'win in strategy,' they [the Iraqis] also lost the power to 'win in battle'."[30] The author argues that the duel over command must precede combat on the ground. More intriguing, the analyst's approach to warfare suggests that information dominance offers the potential to overawe the enemy into surrendering, hence negating the need for actual physical engagement. This type of psychological intimidation through IW—essentially aimed at scaring the enemy into dropping their swords—is deeply embedded in Sun Tzu's philosophy. Strategic advantage (*shih*), a central feature of the *Art of War*, connotes the release of latent energy, both physical and psychological, in order to ride the forces of circumstances to victory. Whether the Chinese genuinely believe that command warfare has eclipsed kinetic force combat remains to be seen.

According to one author, "In waging IW, 'the best combat method is to attack by strategy' . . . to obstruct or upset the enemy's decisionmaking procedure, so as to make the enemy unable to adopt coordinated actions. To be more precise, the main objective of IW is to hit the enemy's cognitive system as well as information system."[31] In terms of the actual application of force, the writer conjures the notion of hitting the enemy's vital points. "The salient feature of IW is that high-precision, high-speed, over-the-horizon attacks become its basic fire application pattern and that the nonstylized 'vital point'-styled structural destruction will replace the traditional-stylized

battles."[32] The author equates the enemy's main vulnerabilities to its ability to process information and make decisions. Identifying, locating, and then attacking such centers of gravity (cognitive and information systems) are central to this concept of IW.

According to the *Liberation Army Daily*, "an attacker can go around the enemy's solid works he has long labored for and, by way of 'surgical removal' and 'digital acupoint pressure' (selective attacks), launch precision raids to destroy the enemy's war resources and shatter his will to resist."[33] Similar to U.S. military thinking, this focus on targeting the opponent's will hints at a very broad conception of IW, including psychological operations. Another writer describes the ability of IW to seek out and destroy the enemy's vital points in much more vivid terms. "Information intensified combat methods are like a Chinese boxer with a knowledge of vital body points who can bring an opponent to his knees with a minimum of movement."[34] A Chinese Defense University publication issued a similar prescription on IW. "Paralyze the enemy by attacking the weak link of his C3I as if hitting his acupuncture point in kungfu combat." The foregoing analyses again suggest that the Chinese believe a successful attack against vital points would cripple the adversary and negate the need to engage in further combat.[35] The notion that centers of gravity, a traditional concept in warfare, might be information-related is a major driving force behind the current debates on the new RMA worldwide. The Chinese have clearly grasped the significance of the relationship between information and center of gravity.

Chinese discussions on IW have centered on the strategy of disrupting the command and control capabilities of the adversary. The literature often presumes that locating and then successfully attacking the enemy's centers of gravity is achievable. Interestingly, this concept of crippling the opponent's ability to act or gain initiative on the battlefield by targeting information systems parallels (if not parrots) the American notion of information dominance, which

overlays traditional kinetic weaponry as a force multiplier. Another subtheme that emerges in the literature is the influence of Chinese strategic tradition. The recurrent notion of attacking the enemy's strategy without actually engaging in combat reflects the indelible imprint of Sun Tzu's philosophy and demonstrates Chinese efforts to internalize IW within a familiar strategic framework. Interestingly, Western militaries, particularly the American armed forces, have also become enamored with Sun Tzu.[36] Beyond the broad strategies that the Chinese have developed, strategists have also distilled very specific conclusions on how IW would be applied in the future.

Chinese Views on IW Capabilities.

Despite the offensive nature of the IW strategies outlined above, the Chinese divide IW into two broad categories of offensive and defensive capabilities. In the offense, IW seeks to attack directly the enemy's information systems. This includes the physical destruction and suppression of the enemy's information operations, such as jamming, weakening, or shutting down the adversary's command and control. Analysts recognize that as China becomes more dependent on IW in future conflicts, Chinese systems would likely be subject to attack as well. Indeed, Chinese observers have scrutinized the Kosovo conflict with great interest to distill lessons learned on potential defensive strategies. Strategists unanimously concur that enhancing resistance to interference and heightening defense against physical attacks are critical requirements for Chinese IW.[37] Defending one's own platforms and ensuring the normal functioning of command and control have become equally important compared to the offense.

Chinese strategists agree that both the offensive and defensive elements of IW require a robust and effective command and control system. IW and any other type of warfare depend on command and control as the architecture and central nervous system. According to one author,

> All activities of information operations are centering around command and control. Command and control cover all areas of information operations and work throughout the whole process of operation, affecting and regulating the overall situation. Any mistakes in command and control will seriously jeopardize an information operation. Therefore, in the study of information operations, we must pay close attention to command and control as the core.[38]

One major objective of C2 is to "obtain timely information, to understand the enemy and ourselves, and to achieve clarity about our situation with great determination."[39] As mentioned above, command and control warfare also seeks to destroy the enemy's ability to acquire, transmit, process, and use information while protecting one's own systems in order to achieve information superiority. For example, command and control systems would coordinate precision strikes and electronic warfare by locating, tracking, attacking, and assessing the damage to enemy targets.

An effective command and control capability requires a wide range of information technologies aimed at increasing the reliability of remote sensing and reconnaissance systems. One author predicts that, "The 21st century will see broad use of high-resolution photography in surveillance satellites, combined air-ground early warning systems for guided missiles, infrared detection systems, deep strike surveillance and control planes, and much use of unmanned reconnaissance planes."[40] The specific tools of offensive and defensive IW include: (1) physical destruction; (2) dominance of the electromagnetic spectrum; (3) computer network warfare; and (4) psychological manipulation. Interestingly, these capabilities almost mirror U.S. doctrine on IW. While the views on specific types of IW differ somewhat between various analysts, several discrete IW applications have dominated recent discourse from the late 1990s to the present. The following briefly discusses the four main aspects of IW:

   • *Precision Strike Warfare*. The Chinese envision "hard" weapons that would physically destroy the enemy's

headquarters, command posts, and C2 facilities. Smart, stealthy, and over-the-horizon weapons would be able to perform precise and "clean" deep strikes. The delivery systems include guided bombs, guided artillery shells, cruise missiles, and antiradiation missiles. Sound waves, electric waves, visible light, infrared waves, lasers, and gases would guide the weapon's sensors.[41]

• *Electronic Warfare*. The Chinese concur that the contest for the electromagnetic spectrum to gain battlefield initiative is a crucial phase of warfare. The objective is to dominate the spectrum while denying the enemy's effective use of electronic equipment. For the offense, one would utilize electronic jamming, electronic deception, directed-energy weapons, and electromagnetic pulse weapons. Hardening of facilities, dispersion, countermeasures, and physical retaliation would constitute the defense. Microelectronics will become a key technological area for investment.[42]

• *Computer Network Warfare*. Chinese strategists cover a wide range of technologies and capabilities in computer warfare. Networked computers would digitize the battlefield, increase the transparency of the battlefield to commanders, and provide real-time data. Computer warfare can manifest itself in more exotic forms such as cyber and hacker wars. Analysts discuss virtual warfare as a means to deceive enemy forces with simulated false commands.[43] Virtual simulations would also prepare Chinese forces prior to actual combat.[44]

• *Psychological Warfare and Deception*. This mode of warfare involves the transmission of information or misinformation to influence the intended audiences' emotions, mode of thinking, and ultimately their behavior. Aimed at both the military and public as the audience, psychological warfare would exert pressure and weaken the enemy's will to carry on the fight.[45] The primary tools include media propaganda (television and radio), leaflet distribution, e-mail, and other forms of communication.

While the existing literature lacks details on specific programs, some recent articles hint at Chinese interest in developing certain technologies, particularly in the areas of remote sensing and reconnaissance. A Chinese researcher at the Huabei Photo-electronics Technology Research Institute offered a rare interview on the military utility of photo-electronics. The researcher outlined various ongoing projects in photo-electronic technologies that would aid China in future conflicts. These include the display of clearer imagery; increase in information transmission speed; higher storage densities; miniaturized photo-electronic devices and systems; and fusion of microwave technologies with photo-electronics.[46]

Another article revealed Chinese interest in airborne and space-based synthetic aperture radar. The system would be used to detect enemy dispositions and to assess battle damage to enemy forces. According to the author, China is expected to launch its first space-based radar in 2003.[47] A *Liberation Army Daily* published an extensive interview with experts on military mapping. This distinguished group of engineers, professors, and researchers discussed remote sensing and navigation satellites; multi-resolution, three-dimensional digitized imagery; and all-weather, real-time reconnaissance capabilities, among other topics.[48] Clearly then, remote sensing and reconnaissance, a central component of modern command and control, have attracted increasing attention within the Chinese scientific and defense communities.

A Preliminary Evaluation of Chinese IW Literature.

While China's IW literature and American interpretations of Chinese writings cover a broad range of concepts and capabilities, most analyses lack concrete evidence on the future direction of Chinese IW. Chinese IW doctrine and force structure have remained frustratingly elusive. The writings often theorize on the benefits of IW and tend to present a wish list of capabilities that the

Chinese hope to acquire. These abstractions reveal the extent to which the Chinese are still struggling with a highly amorphous and ill-defined concept in warfare. However, some preliminary assessments can be made about the existing literature on IW.

Are the Chinese Copy Cats? As noted earlier, Chinese interpretations of IW dovetail closely with the notion of information dominance in American military doctrine. In many cases, the Chinese have borrowed heavily from (and even outright plagiarized) open literature and security debates within the United States.[49] Mulvenon identifies several Chinese writings that are virtually identical to the U.S. Air Force's "Six Pillars of IW" and *Joint Vision 2010*. For example, one author's definition of IW as "electronic warfare, tactical deception, strategic deterrence, propaganda warfare, psychological warfare, computer warfare, and command and control warfare" mirrors the Air Force's conception of IW.[50] The Chinese have also translated in full the *Joint Doctrine for Command and Control Warfare* (JP3-13.1) and Field Manual (FM)-100-3.[51] This peculiar tendency to reproduce American doctrine further evidences the daunting theoretical and analytical difficulties that the Chinese have encountered in studying IW. Indeed, this phenomenon of intellectual imitation is highly reminiscent of Soviet literature on nuclear strategy and doctrine in the 1960s and 1970s.[52] If the Chinese are merely mimicking American discourse, then the writings further obscure China's real intentions and capabilities in IW. More importantly, the intellectual debates raging in the United States are simply incompatible with the current capabilities and needs of the Chinese. The primitive critical infrastructure in China, while rapidly expanding in recent years, is not nearly as vulnerable as the American counterpart. The Chinese also do not have the advanced systems to conduct offensive IW on the scale of the United States.

Why, then, are the Chinese engaged in a potentially fruitless exercise? It may be that China is simply extracting

the benefits and lessons from the American experience in IW through imitation. However, such a conclusion would be an oversimplification of Chinese realities that could cloud better understanding of China's developments in IW. In the preface of *China Debates the Future Environment*, Michael Pillsbury points to a prominent and recurring problem in the American study of Chinese security policy:

> Some Americans wrongly believe Chinese views reflect a mirror image of their own. This study suggests instead that the Chinese have their own unique perceptions, which may be difficult to appreciate.
>
> The risk of mirror imaging our own views was an issue also present in the study of the Soviet Union. Andrew Marshall, Director of the Office of Net Assessment, cautioned against assuming that a foreign nation's strategic assessment is merely a reflection of America's: "Soviet calculations are likely to make different assumptions about scenarios and objectives . . . perform different calculations, use different measures of effectiveness, and perhaps use different assessment processes and methods. The result is that Soviet assessments may substantially differ from American assessments." Marshall's cautionary note also applies to understanding Chinese assessments of the future.[53]

The study of Chinese IW could similarly succumb to such temptations of mirror imaging. The following analysis suggests some probable explanations as to why Chinese strategists have so assiduously copied American literature on IW.

The Chinese may have fallen prey to the intellectual "noise" generated within the United States. In an environment where the free flow of ideas, both good and bad, is encouraged and valued at a premium, the American system often produces an over abundance of information. As Greg Rattray illustrates, the entire array of conceivable institutions on national security, ranging from the military services to think tanks to commissions mandated by the president, have all chimed in on IW.[54] Each of these bodies has also prescribed a dizzying set of responses and policies

in conducting IW.[55] As one American columnist recently commented on the Bush administration's mixed signals on U.S. policy toward Taiwan, "Cacophony in the form of conflicting statements is America's most effective form of disinformation."[56] The Chinese may have convinced themselves that the euphoric descriptions of "full spectrum dominance," "information superiority," or "system of systems" are genuinely accepted in the United States as truisms or have been achieved.[57] For example, an analyst at the Chinese National Defense University examining the U.S. Joint Chiefs of Staff's *Joint Vision 2020* believes that the United States will achieve "all-round information superiority" as touted by the document and warns that China should maintain vigilance to counter such a hegemonic trend.[58] Accepting America's apparent ability to achieve such ambitious (if not questionable) military capabilities at face value risks under-rating China's own potential.

Another more ominous explanation of China's apparent acceptance of American IW discourse at face value is that the effort is deliberately intended to mislead the audience in the United States. Indeed, it is entirely conceivable that the Chinese government may be releasing some of the current IW discussions in an extensive deception campaign. China may believe that by actively fostering a burgeoning literature on IW, the outside world would be convinced that the PLA is vigorously pursuing the formidable potential of IW. Such a calculated strategy could be intended to unnerve potential adversaries, disguise China's actual intentions and growing capabilities to maximize the element of surprise, or to hide Chinese weaknesses and vulnerabilities in IW. Beijing's successes in whipping up nationalistic fervor among the public through the state-controlled media in the aftermath of the accidental Belgrade embassy bombing and the April 2001 reconnaissance plane accident highlight China's ability to centrally orchestrate and manage domestic and foreign perceptions. Turning the previous point on its head, the Chinese may be generating

21

their own set of intellectual "noise" to confuse and to keep American defense planners off-balance. The diplomatic maneuvers and the public relations contest between the United States and the Soviet Union in the early years of the space race provide a vivid historical example of mutual noise making. Khrushchev repeatedly exaggerated the capabilities of the Soviet space program to boost the Soviet Union's (and his own) image.[59] The Soviets also deliberately overstated the advances in strategic arms in order to disguise the actual inferiority of their forces.[60]

This deception effort is only possible given the authoritarian nature of the regime and the relative insularity of Chinese society. However, China is undergoing rapid social and economic change that has gradually undermined the capacity of the authorities to control the flow of ideas. For example, while heavily monitored by Chinese authorities, the proliferation of Internet access has opened a potential new avenue for bypassing government control over information. The flourishing publishing businesses not under direct government control have also produced many controversial works that would have been unthinkable a decade ago. For example, the release of *Unrestricted Warfare*[61] (through a semi-independent publishing house) caused a major sensation in Washington.[62] The authors, two PLA senior colonels, advocated the indiscriminate use of military and nonmilitary means to attack the United States during conflict. The publisher's affiliation with the PLA suggested that at least some elements of the military leadership endorsed the radical ideas contained in the book. Interestingly, the publication also spurred an intense and often divisive debate in China's military circles. There were fears that the authors may have divulged too much information on Chinese thinking to the outside world.[63] In short, China's gradual internal opening will curtail the government's ability to influence the media. However, as China's blatant news manipulation in the aftermath of the April 2001 spy plane incident revealed, the

state-controlled media's impact will still be felt in Chinese society for some time to come.

Falling in Love with the "Information Edge." The IW writings clearly demonstrate the powerful conviction among Chinese analysts about the power of information. The literature tightly fuses the accumulation of knowledge with military success. Indeed, some authors describe the relationship between information aided by advanced technologies and victory almost in absolute terms. Many writers declare that the accretion of knowledge and early preparations would make victory inevitable. In other words, information power determines the outcomes of wars. The recurring references to the dictum that proper knowledge would obviate the need to engage in actual combat demonstrate the profound influence of Sun Tzu's philosophy. Moreover, there is an implicit and prevalent assumption in the analyses that such knowledge is attainable both prior to and during war. In short, the ability to gather and process information appears to have become a panacea in warfare for many Chinese IW strategists. This belief in knowledge follows closely with Admiral William Owen's concept of a system of systems. He declares, "when technology is correctly applied to the traditional military functions—to see, to tell, and to act—a powerful synergy is created, producing an effect much greater than the sum of the components."[64] Premised on the power of information technologies, he argues that "dominant battlespace knowledge," "near-perfect mission assignment," and "immediate/complete battlespace assessment" would create the requisite conditions for victory.

What does not appear in the Chinese literature (and Owen's work) regarding knowledge and information is equally instructive. Most analysts generally ignore the harsh reality that data is not always accessible or perfect. Accumulation of knowledge particularly under the duress of war is often a haphazard and unreliable exercise. Indeed, the accidental bombing of the Chinese embassy in Belgrade in 1999 should have demonstrated quite clearly that even

the most sophisticated military power remains subject to the Clausewitzian fog of war. Beijing's stubborn conviction that the bombing was not an accident may in part reflect Chinese illusions that technology does have the power to lift the fog (although the real motive for the diplomatic bluster may well be to extract political capital from the incident). On a related point, most IW strategists tend to skirt the practical application and hence the limitations of IW. Chinese analysts do not discuss how one gathers, analyzes, and disseminates information as a process. They similarly exclude from their analyses the difficulties in assessing and verifying data. The ability to harness knowledge is simply accepted at face value as the solution to eliminating uncertainty in war and the key to victory.

What accounts for this apparent blind faith in information? First, Sun Tzu's influence as a strategic tradition remains very palpable. The literature survey for this monograph demonstrates that the notion of winning without fighting through superior knowledge is highly appealing as a theoretical concept. Second, given that the current discussions are conceptual exercises, most of the writings understandably focus on the abstract and the most ideal situations for information war. This tendency to describe IW within the vacuum of theory often has the effect of exaggerating the power of knowledge. Third, the defense community in China remains deeply divided over the future form of warfare. IW advocates must contend with supporters of the traditional people's war concept, still a dominant force in the PLA, and the more conventional high-tech warfare school of thought.[65] As representatives of a tiny minority view, they must present their case in the most favorable terms. Hence, radical thinkers (like Owens) are naturally compelled to promote the highly appealing notion that knowledge will make winning without fighting possible. The emergence of internal debates and political infighting owing to the introduction of new concepts and technologies is a prevalent if not inevitable phenomenon in any defense community around the world. New ideas often

challenge the entrenched interests of military organizations, which are by nature conservative and resistant to radical change. Authors sometimes must produce provocative writings in order to propel the debate in the hopes of breaking the status quo or changing the existing order. The current literature on Chinese IW is clearly no exception. Regardless of which explanation is preferred for it, the general acceptance that knowledge is the key to mastering IW could have direct consequences for Chinese developments in IW.

Forgetting Clausewitz. Chinese writings on IW ignore the inherently interactive nature of combat. The ability to gather and utilize knowledge is always seen from the perspective of the self rather than from the enemy's position. It assumes that the enemy does not enjoy the same type of access to information or has not devised parallel IW strategies. In concrete terms, "The notion that one can expect to attack an enemy's satellite and computer networks while the enemy will not have thought to do so against oneself, or that the enemy will not have tried to take precautions against such an attack, is dangerously naïve."[66] The failure to appreciate the enemy's IW strategies could magnify the problems that result from an unquestioning faith in knowledge as mentioned previously. The assumption that the adversary has not devised counter measures to deceive, mislead, or misinform could lead to disastrous consequences. It might inflate Chinese confidence in their ability to gather and process accurate information about the enemy and thereby open themselves to terrible blunders or miscalculations.

In *Keeping the Edge*, Victor A. DeMarines highlights the inherent interactive nature of cyber information operations:

> A difficulty inherent in CND [Computer Network Defense] is that the attacker has the initiative, and the defender cannot know the time and place of the next attack . . . A critical characteristic of CNA [Computer Network Attack], which creates numerous problems in planning its use, is its fragility. Many forms of CNA are most effective when the enemy does

not realize that it is under attack, because they can readily be countered once the enemy knows exactly how the attack is being carried out.[67]

In other words, computer network attack or defense, while highly appealing, are fraught with uncertainty. Without careful planning with the enemy constantly in mind, the attack could be ineffective or the defense could be circumvented by deception and surprise.

DeMarines also comments on the dilemmas that the policymaker faces when employing computer network defense or attack:

> There is an inherent conflict between the requirements for effective CND and the requirements for CNA. This conflict arises whenever we discover a potential vulnerability in a computer network. If we keep this vulnerability secret, and if a future enemy does not independently discover the vulnerability and protect against it, then we can exploit it for CNA. But if we develop a defense against the vulnerability and deploy it widely in our networks, we make it highly likely that the future enemy will learn about the vulnerability and the defense, and we will be unable to use it for CNA. However, if a future enemy discovers this vulnerability independently, and we have done nothing to protect our own networks against it, the enemy can use it to attack us.[68]

The complex interactive process in IW means that the action taken by one side could potentially be negated immediately if the adversary is alert or aware. The linear approach to IW that the Chinese appear to have adopted ignores the Clausewitzian implications of a duel between two opposing forces.

The Ghost of Sun Tzu Still Lingers. The presence of Sun Tzu's philosophy is inescapable in the IW literature. As noted earlier, Sun Tzu's notion of winning without fighting and attacking the enemy's strategy (command and control systems) resonates powerfully with Chinese strategists. In addition, Chinese discussions of IW as a tool for deception carry a distinct overtone of Sun Tzu's influence. As

suggested above, Sun Tzu's philosophy tends to reinforce an unwarranted perception among Chinese commentators that knowledge or information can become a panacea in warfare. In short, traditional frameworks for understanding strategy could have a distorting affect on Chinese views of IW. However, some observers have concluded that China's strategic culture might in fact help the Chinese benefit more from IW than the West. According to an early study on Chinese IW, "Despite our technological edge, we in the West may have much to learn from Chinese views of conflict in the information age. Indeed, Sun Tzu, with his emphasis on the power of 'knowing', may be more relevant in the future than Clausewitz, for whom 'friction', not information, was of overarching importance."[69] They suggest that this cultural difference may in fact enable China to achieve high levels of sophistication faster and earlier than Western analysts have generally predicted.

Whether Chinese strategists have something useful to contribute analytically by looking through the lens of Sun Tzu or whether they have deluded themselves into accepting the capacity of information power to lift the fog of war remains to be seen. However, China's ancient strategic culture, which is deeply imbedded in contemporary strategic thinking, will likely impact the future direction of Chinese IW. More specifically, a combination of practical considerations and strategic traditions will determine the course and uniqueness of China's IW program. Notwithstanding the steady boosts in defense spending, China's military establishment still faces severe resource constraints. In light of the economic uncertainty in the coming years, China would not attempt or be able to duplicate American efforts in IW. Moreover, Chinese weakness in conventional capabilities vis-à-vis the United States will force the PRC to focus on asymmetric strategies, which might involve certain aspects of IW (although the specifics remain unclear). In addition, Mao's people's war tradition and Sun Tzu's philosophy will likely exert both conscious and subconscious influences on Chinese thinking

27

on IW. For example, denial and deception and the notion of fighting from a position of weakness will undoubtedly dominate much of the discourse. Regardless of which elements of IW Beijing choose to exploit, the Chinese will likely pursue their own brand of IW that could deviate radically from Western conceptions and models. The pursuit of a unique IW strategy, which would not likely be well understood in the West, could be a perfect formula for achieving surprise (or abysmal failure) against China's adversaries.

How Different from American Thinking? The literature suggests that Chinese strategists tend to conceptualize IW in the broadest terms possible. Similar to U.S. thinking, the Chinese expand IW to the psychological realm. However, strategists broaden IW attacks beyond warfighting purposes. They often discuss attacking the adversary's social, economic, and internal political structures. According to one analyst, "The soul of informationized warfare is to 'subdue the enemy force without battle.' Its essence is to force the opponent to give up the wish to resist and thereby to end confrontation and stop fighting by ultimately attacking their perception and belief, using information energy as the main means of action."[70] The Chinese essentially hope to elevate IW to a higher level of operational military art form. These strategists believe that by tapping into the enemy's thought processes, values, and motives one can identify, manipulate, and reduce the adversary's will to resist and hence achieve victory without actual combat. In concrete terms, IW attacks intended to inflict pain on the adversary's society might be employed to impact public opinion and increase the political costs of fighting against China (much like the use of strategic airpower during World War II). The Chinese could direct IW against America's increasingly vulnerable and sprawling critical infrastructure in order to complicate Washington's decisionmaking process. The Chinese could apply indirect pressure on certain segments of the American population to induce broader public panic in the hopes of reducing

Washington's political will to act in the event of crisis. For example, consider the potential impact of tainting processed food by infiltrating the manufacturing process via computers.[71] Whether the Chinese would take such action without fear or in spite of potential American retaliation and escalation will be the subject of analysis in the following section.

In any case, it is clear that an assessment of Chinese IW literature produces more questions than answers. Whether the Chinese have reached the wrong conclusions on IW within their unique political context remains unclear. Whether certain aspects of the literature are intended to mislead the outside world is equally unanswerable. The environment of rapid change and innovation inherent to information technologies compounds the uncertainties. Moreover, China confronts the United States, its designated potential adversary, who holds a dauntingly tremendous lead. Chinese analysts are constantly bombarded by the seemingly endless production of American analysis on IW. The confluence of all these factors may have shaped the sweepingly ambitious—and at times seemingly unrealistic or naïve—analysis of IW among Chinese strategists.

Assessing the Chinese IW Threat to the United States.

Given the intense Chinese interest in IW, China will likely devote substantial resources to studying the use of and acquiring state-of-the-art information technologies. In particular, China will seek capabilities that would help gather, process, and exploit information on the battlefield to establish an information-based military force. Command and control systems, such as reconnaissance satellites and surveillance systems will become important elements in China's force structure. Moreover, as a "latecomer" to the information revolution, China may be able to reap the hard-earned fruits of nations that pioneered IW warfare.

29

The diffusion and availability of technologies could allow China to leapfrog generations of obsolescent technologies within the Chinese force structure.

Beyond the technological implications, future developments in IW could have broader effects on Chinese policy and strategy. Unfortunately, predicting the future path of Chinese IW remains a haphazard exercise. As noted above, the current Chinese literature itself reveals a yawning gap between theory and practice. Since China is notorious for shrouding any shred of data on defense capabilities in absolute secrecy, it is unclear how the Chinese might apply newly acquired IW capabilities. This level of uncertainty on when and how China would master IW adds greater urgency to understanding Chinese strategic thought on IW.

One of the enduring puzzles is how China might employ IW in the event of crisis involving the United States. An area that deserves close study is the apparent attraction among Chinese strategists to IW as a preemptive weapon. Chinese strategists uniformly recognize that they are likely to fight from a position of weakness. Hence when a conflict with a superior foe occurs, China must seek to achieve its political objectives while precluding an actual clash of arms that would likely result in defeat. The literature suggests strongly that IW capabilities might provide the "silver bullet" for such a scenario. In essence, these strategists are exploring IW as a tool to preempt conflict by attacking and crippling the enemy's vital points (command and control systems) in order to reduce the adversary's will to fight at the very outset of war. Again, this concept dovetails closely with Sun Tzu's dictum of winning without fighting and Mao's people's war concept of overcoming the superior with inferior forces.

Mulvenon argues that the Chinese obsession with IW as a preemptive weapon pose the most worrisome and unpredictable policy challenge for the United States. He paints a stark scenario:

30

When one imagines scenarios in which the PLA would be concerned with preemptively striking U.S. forces during the deployment phase for early strategic victory, it is difficult to avoid the obvious conclusion that the author is discussing a Taiwan conflict. For the PLA, using IW against U.S. information systems to degrade or even delay a deployment of forces to Taiwan offers an attractive asymmetric strategy. American forces are highly information-dependent, and rely heavily on precisely coordinated logistics networks . . . If PLA information operators using PCs were able to hack or crash these systems, thereby delaying the arrival of a U.S. carrier battle group to the theater, while simultaneously carrying out a coordinated campaign of short-range ballistic missile attacks, "fifth column," and IW attacks against Taiwanese critical infrastructure, then Taipei might be quickly brought to its knees and forced to capitulate to Beijing.[72]

Mulvenon notes that the incentives for employing such a strategy are three-fold. First, the proliferation of information technologies enables China to gain access to and develop such capabilities in a relatively short period of time, especially when compared to a full-fledged conventional buildup. Second, IW negates the need to use China's precious few air and naval assets for an invasion campaign or massive attack against Taiwan, both of which would likely result in severe Chinese losses or failure for at least the next 10 years. Finally, IW, if sophisticated enough, could create adequate levels of plausible deniability. Mulvenon concludes that, "IW may currently offer the PLA some attractive asymmetric options, some of which may be decisive in *narrowly circumscribed situations* [emphasis added]."[73]

Despite its theoretical appeal, preemption as an IW strategy represents a double-edged sword. As Mulvenon suggests, under certain circumstances, IW could lead to decisive results. However, in the worst-case scenario, preemption could be highly destabilizing and escalatory. As Rattray argues, an escalatory response from the United States is possible should the damage to U.S. critical infrastructures prove to be extensive.[74] Is it likely then, for

China to unleash an IW attack that could invite escalation in kind? If Beijing does intend to preclude U.S. intervention in a Taiwan crisis, it is entirely conceivable that China and the United States might find themselves in a dangerous tit-for-tat face off. To successfully preempt an opponent, the strike must be decisive and overwhelming. Once such powers of IW are unleashed in a preemptive attack, the ability to control and calibrate forces becomes extremely difficult. Indeed, de-escalation may not be an option once the Chinese order such an IW attack. Decisiveness of this kind requires almost near-perfect knowledge of the enemy and a very high degree of confidence in the ability to successfully destroy the adversary's vital points (both extremely questionable propositions). Should such a high risk attack fail due to faulty information or prudent anticipation on the part of the adversary, the enemy may not be deterred and may respond with even greater force. Rather than the deterrent effect expected from IW (much as the Japanese planners of the surprise attack against Pearl Harbor had hoped), a reckless application of information operations could provoke massive retaliation.

The literature survey on Chinese views of IW and its convergence with preemption also leads to some other unsettling conclusions. Notably, the apparent belief that information is a panacea in warfare could breed dangerous attitudes. In the tradition of Sun Tzu, Chinese analysts of IW assert that knowledge can be assembled together in a rational and coherent manner that would produce inevitable victory. The assumption that superior information can overcome the fog of war could encourage the Chinese to devise ambitious IW strategies that might backfire terribly when employed. For example, confidence in attaining accurate knowledge prior to war and the emphasis on preplanning often leads to inflexibility. As John Keegan persuasively argued, the faith in war plans among the belligerents of World War I led to what he called "a tragic and unnecessary conflict."[75] Those war plans meticulously laid out a very specific course of action that

brooked little deviation. The underlying assumption was that proper information and planning would determine the outcome of wars. Indeed, all the plans anticipated quick victories in a short war. The actual course of events led to prolonged stalemate and mass slaughter. Europe's hubris at the time could similarly infect Chinese defense planners.

It is clear then, that the use of IW for preemptive purposes could be highly escalatory and unstable in crisis situations. The consequences of such a strategy could be dangerously explosive, particularly in a conflict involving the United States over a Taiwan crisis. This extreme scenario of course assumes that the Chinese IW strategy actually works. Beijing may also be equally unable to cope with a massive and complete failure to achieve its political objectives through IW. Given that an "IW Pearl Harbor" remains untested and the means to assess damage are underdeveloped and inherently difficult, it is entirely possible that the attack would end in a pathetic fizzle. China's reliance on IW to conduct warfare at the expense of other traditional capabilities could lead to a multitude of unintended consequences.

If on the other hand, the Chinese are acutely aware of the counter productive and possibly disastrous results of an IW Pearl Harbor, they may be self-deterred from exercising such an option. Is Chinese IW as an asymmetric threat therefore a phantom menace? To what extent should the uncertainty and ambiguity of the Chinese threat dictate how the United States responds to China's IW developments? Examining and weighing the likelihood of Beijing resorting to IW against the United States is therefore a policy-relevant and extremely elusive task. Greg Rattray's formula for understanding strategic IW is a useful model for assessing the Chinese IW threat to the United States. Rattray states, "Despite the availability of technological tools for digital warfare, the utility of engaging in strategic IW for U.S. adversaries will vary based on their political objectives, likely campaign strategies, and willingness to risk retaliation and

escalation."[76] He outlines four conditions for achieving success in strategic warfare: (1) offensive advantage; (2) significant vulnerability of centers of gravity to attack; (3) minimal prospects for retaliation and escalation; and (4) identifiability and targetability of enemy vulnerabilities and assessibility of damage inflicted. Rattray argues that strategic IW can only reasonably achieve an offensive advantage. Given the uncertainties surrounding the probability of success in employing IW, the Chinese might also be constrained by these considerations.

Does this mean that China is not likely to employ IW? A Chinese decision to use IW will depend on Beijing's perceptions of the external security environment and internal politics. As Rattray argues, the broader political context is the central starting point for understanding IW. Clearly, Beijing would not likely use IW to reinforce its territorial sovereignty over Tibet. However, on an issue as explosive as the fate of Taiwan, self-deterrence could come under severe strain. Therefore, the United States cannot assume that since the Chinese face similar strategic and operational constraints in the use of IW that Beijing will be dissuaded from taking a risky course of action. Indeed, if the stakes are high enough, such as losing Taiwan and, in the process, destroying the Communist Party's legitimacy, the Chinese might be more tolerant of failure and/or escalation. If a desperate Chinese leadership is sufficiently convinced that they no longer have anything to lose from taking action, reliance on IW as a preemptive "use it or lose it" option may not seem so unattractive or dangerous. While the probability of China using strategic IW is low at present or in the short-term, the political context may change sufficiently in the future to warrant caution and preparation on the part of the United States.

We've Only Just Begun.

The policy implications in this analysis are clearly less than sanguine. However, it is important to note as a caveat

that the lack of reliable sources and the opaqueness of China's defense community preclude sufficient certainty on the future direction of Chinese IW. As suggested above, the Chinese may simply be following a familiar U.S.-Soviet pattern of rhetorical theatrics. The Chinese are still grappling with a nascent concept that even the most developed countries are also struggling with. Moreover, China's capabilities are still too primitive to compete against advanced military powers such as the United States. In short, China will not be able to achieve the much touted information dominance for some time to come.

However, it would be dangerous and naïve to simply disregard the potential Chinese threat. Historically, the concept of offensive IW has been a tightly held secret even within the United States itself. The seemingly excessive secrecy surrounding offensive capabilities has three root causes. First, the United States kept this concept secret in deference to the political sensitivities among allies. Second, there were fears that touting offensive IW might engender enmity on the part of adversaries in an act of self-fulfilling prophesy. Third, as mentioned before, the frailties of offensive and defensive IW strategies make them vulnerable to countermeasures. Hence, even the most transparent countries developing IW have been very reluctant to reveal their strategies and capabilities. In other words, the lack of evidence on IW has no bearing on whether it exists or not or whether the country is proficient at it or not.[77] China is no exception.

As a final cautionary note, the oftentimes reflexive response among some scholars to discount discussions of the "China threat" as mere paranoia or hawkishness must be tempered with some historical perspective. In many ways, the post-Cold War period resembles the interwar interregnum, during which military powers experimented with new technologies, organizations, and doctrine. As World War II approached, the balance of forces heavily favored the Allied powers. The political will of the leadership and the public mood in London and Paris had

35

shifted from reluctance to surprising enthusiasm to fight. In contrast, Nazi Germany did not field the best or the most advanced military hardware. Yet, the hand wringing, bumbling generals led by a madman and backed by a German public with little appetite for war unleashed the blitzkrieg that would shatter the French and British forces in less than 7 weeks. How could this have happened? In *Strange Victory*, Ernest May argues convincingly that the devastating defeat resulted from the Allied failure to anticipate German plans and to appreciate the magnitude of British/French miscalculations. He concludes:

> In sum, the essential thread in the story of Germany's victory over France hangs on the imaginativeness of German war planning and the corresponding lack of imaginitiveness on the Allied side. Hitler and his generals perceived that the weakness of their otherwise powerful enemies resided in habits and routines that made their reaction times slow. They developed a plan that capitalized on this weakness. French and British leaders made no effort to understand how or why German thinking might differ from theirs. They neglected to prepare for the possibility of surprise, and, as German analysts and planners predicted, they could not react promptly once events began to be at odds with expectations.[78]

The lesson from this analysis is that constant vigilance is the only answer to avoiding ugly surprises. Further analysis is clearly required but this preliminary study suggests that China's evolving attitudes toward IW could pose an increasingly daunting and unpredictable challenge for American policymakers.

ENDNOTES

1. James Adams, "Virtual Defense," *Foreign Affairs*, Vol. 80, No. 3, May/June 2001, pp. 100-101.

2. The Joint Staff, *Enabling the Joint Vision*, Washington, DC: The U.S. Department of Defense, May 2000; Chairman of the Joint Chiefs of Staff, *Information Operations: A Strategy for Peace . . . The Decisive Edge in War*, Washington, DC: U.S. Department of Defense, March 1999, p. 3.

3. Chairman of the Joint Chiefs of Staff, *Joint Vision 2020*, Washington, DC: U.S. Department of Defense, June 2000, p. 28.

4. Chairman of the Joint Chiefs of Staff, *Joint Vision 2010*, Washington, DC: U.S. Department of Defense, July 1997, p. 16.

5. Assistant Secretary of Defense for Command, Control, Communications, and Intelligence, *Information Superiority: Making the Joint Vision Happen*, Washington, DC: U.S. Department of Defense, 2000, p. 5.

6. *Information Operations*, pp. 10-11.

7. Kate Farris, "Chinese Views of Information Warfare," *Defense Intelligence Journal*, Vol. 10, No. 1, Winter 2001, p. 38.

8. *Ibid.*, p. 37.

9. Michael Pillsbury, *China Debates the Future Security Environment*, Washington, DC: National Defense University Press, 2000, pp. 3-61. Sponsored by Andrew Marshall's Office of Net Assessment, this landmark study is a comprehensive analysis and synthesis of over 200 Chinese writings published from 1994-99. The Chinese authors are mostly from prestigious government-funded research institutes.

10. Kenneth F. McKenzie, Jr., *The Revenge of the Melians: Asymmetric Threats and the Next QDR*, Washington, DC: Institute for National Strategic Studies, National Defense University, 2000) 1-2.

11. Pillsbury, *China Debates*, p. 286.

12. June Teufel Dreyer, *The PLA and The Kosovo Conflict*, Carlisle Barracks: U.S. Army War College, Strategic Studies Institute, May 2000, pp. 12-15.

13. Bruce D. Berkowitz and Allan E. Goodman, *Best Truth: Intelligence in the Information Age*, New Haven: Yale University Press, 2000, pp. 14-15.

14. Martin Van Creveld, *Command in War*, Cambridge, MA: Harvard University Press, 1985, p. 4.

15. *Ibid.*, p. 5.

16. Liu Huaqing, "Unswervingly March Along the Road of Building a Modern Army With Chinese Characteristics," *Jiefangjun Bao*, August 6, 1993, in *FBIS-CHI*, November 20, 1996.

17. Wang Baocun, "Information Warfare in the Kosovo Conflict," *Jiefangjun Bao*, May 25, 1999, in *FBIS-CHI*, June 23, 1999; and Yao Yunzhu, "Federal Republic of Yugoslavia Crisis Shows Need to Strengthen PLA: Discussion of the Kosovo Crisis Among Experts and Scholars," *Jiefangjun Bao*, April 13, 1999, in *FBIS-CHI*, April 28, 1999.

18. James Mulvenon, "The PLA and Information Warfare," in *The People's Liberation Army in the Information Age*, James Mulvenon and Richard H. Yang, eds., Washington, DC: RAND, 1999, p. 178.

19. Pillsbury, *China Debates*, p. 264.

20. *Ibid.*, p. 286.

21. Ch'en Huan, "The Third Military Revolution," in *Chinese Views of Future Warfare*, Michael Pillsbury, ed., Washington, DC: National Defense University Press, 1997, p. 389.

22. Hai Lung and Chang Feng, "Chinese Military Studies Information Warfare, *Kuang Chiao Ching*, January 16, 1996, in *FBIS-CHI*, February 21, 1996, pp. 33-34.

23. You Ji, "The Revolution in Military Affairs and the Evolution of China's Strategic Thinking," *Contemporary Southeast Asia*, No. 21, December 1999, p. 351.

24. Michael Pillsbury, "Chinese Views of Future Warfare," in *China's Military Faces the Future*, James R. Lilley and David Shambaugh, eds., Washington, DC: American Enterprise Institute, 1999, p. 69.

25. John Arquilla and Solomon M. Karmel, "Welcome to the Revolution . . . in Chinese Military Affairs," *Defense Analysis*, Vol. 13, No. 3, December 1997, p. 259.

26. Wang Baocun and Li Fei, "Information Warfare," in *Chinese Views of Future Warfare*, Michael Pillsbury, ed., Washington, DC: National Defense University Press, 1997, p. 328.

27. Mulvenon, p. 180.

28. According to *Joint Vision 2010*, information superiority is defined as: "the capability to collect, process, and disseminate an

uninterrupted flow of information while exploiting or denying an adversary's ability to do the same."

29. Huang Youfu, Zhang Bibo, and Zhang Song, "New Subjects of Study Brought About by Information Warfare," *Jiefangjun Bao*, November 11, 1997, in *FBIS-CHI*, December 20, 1997, p. 3.

30. *Ibid.*

31. Shen Weiguang, "Checking Information Warfare—Epoch Mission of Intellectual Military," *Jiefangjun Bao*, February 2, 1999, in *FBIS-CHI*, February 15, 1999, p. 5.

32. *Ibid.*

33. "Where Should Attention be Focused in Preparing for Military Struggle," *Jiefangjun Bao*, July 25, 2000, in *FBIS-CHI*, July 25, 2000, p. 3.

34. Chang Mengxiong, "Information Intensified—A Mark of 21st Century Weapons and Military Units," *Guoji Hangkong*, March 5, 1995, in *FBIS-CHI*, March 5 1995, p. 5.

35. Chong-Pin Lin, "Info Warfare Latecomer," *Defense News*, April 12, 1999, p. 23.

36. In the United States, the National Defense University (NDU), the service schools, and the command and staff colleges all teach the *Art of War* as a part of the core curriculum. See NDU course description of Fundamentals of Military Thought and Strategy at *http://www.ndu.edu/ndu/nwc/AY00/5602SYL/Topic10.html*. Recently, the Institute for National Strategic Studies at NDU dedicated its 1997-98 annual writing competition on information warfare to Sun Tzu. See introduction to the research competition at *http://www.ndu.edu/inss/siws/intro.html*.

37. Wang Pufeng, "The Challenge of Information Warfare," in *Chinese Views of Future Warfare*, Michael Pillsbury, ed., Washington, DC: National Defense University Press, 1997, pp. 322-323.

38. Yuan Bangen, "Setting Eyes on Development, Stepping Up Research in Information Warfare Theories and Construction of Digital Forces and Digital Battlefields," *Zhongguo Junshi Kexue*, February 20, 1999, in *FBIS-CHI*, July 6, 1999, p. 4.

39. Wang Baocun and Li Fei, p. 320.

40. Xie Guang, "Year-end Report: Wars Under High-Tech," *Renmin Ribao*, December 27, 1997, in *FBIS-CHI*, January 30, 2000, p. 2.

41. Wang Baocun and Li Fei, p. 332.

42. Wang Baocun, "A Preliminary Analysis of Information Warfare," *Zhongguo Junshi Kexue*, November 11, 1997, in *FBIS-CHI*, March 29, 1998, p. 3.

43. Major General Dai Qingmin, "Innovating and Developing Views on Information Operations," *Zhongguo Junshi Kexue*, August 20, 2000, in *FBIS-CHI*, September 11, 2000, p. 10.

44. Zeng Sunan and Zhu Xiaoning, "Virtual Reality: An Important Medium in Theoretical Innovation," *Jiefangjun Bao*, May 16, 2000, in *FBIS-CHI*, May 16, 2000.

45. Xu Hezhen, "Focus on Psychological War Under the Background of Larger Military Strategy," *Zhongguo Junshi Kexue*, October 20, 2000, in *FBIS-CHI*, December 11, 2000, p. 11.

46. Xu Dexin, "Military Photo-electronics Technology," *Kexue Shibao*, June 6, 1999, in *FBIS-CHI*, September 14, 1999, pp. 1-3.

47. Zhang Zhizhong, "Remote Sensing Application Techniques," *Huokong Leida Jishu*, March 1, 2000, in *FBIS-CHI*, October 16, 2000, p. 4.

48. "Experts Discuss Military Mapping Support in Information Era," *Jiefangjun Bao*, May 17, 2000, in *FBIS-CHI*, May 17, 2000, pp. 1-5.

49. Mulvenon, p. 182.

50. Su Enze, "Logical Concepts of Information Warfare," *Jiefangjun Bao*, March 19, 1996.

51. Mulvenon, p. 181.

52. Nikolai Sokov, *Russian Strategic Modernization: The Past and Future*, New York: Rowman & Littlefield Publishers, 2000, p. 34.

53. Michael Pillsbury, *China Debates*, No. xv, cites Andrew W. Marshall, "A Program to Improve Analytic Methods Related to Strategic Forces," *Policy Sciences*, November 1982, p. 48.

54. Greg Rattray, *Strategic Warfare in Cyberspace*, Cambridge, MA: MIT Press, 2001, pp. 8-14.

55. *Ibid.*, pp. 314-342.

56. Jim Hoagland, "Creating a New Tone," *Washington Post*, April 29, 2001, p. B-7.

57. See Admiral William Owens and Ed Offley, *Lifting the Fog of War*, New York: Farrar, Straus and Giroux, April 2000; or Joseph S. Nye and William A. Owens, "America's Information Edge," *Foreign Affairs*, Vol. 75, No. 2, March/April 1996, pp. 20-36. See also Chairman of the Joint Chiefs of Staff, *Joint Vision 2020*, Washington, DC: U.S. Department of Defense, June 2000; The Joint Staff, *Enabling the Joint Vision*, Washington, DC: The U.S. Department of Defense, May 2000; Chairman of the Joint Chiefs of Staff, *Information Operations: A Strategy for Peace . . . The Decisive Edge in War*, Washington, DC: U.S. Department of Defense, March 1999; Assistant Secretary of Defense for Command, Control, Communications, and Intelligence, *Information Superiority: Making the Joint Vision Happen*, Washington, DC: U.S. Department of Defense, 2000; and The Joint Staff, J-6, *Information Assurance through Defense in Depth*, Washington, DC: U.S. Department of Defense, February 2000.

58. Cui Shizeng, "Reading the US Military's Joint Vision 2020," *Jiefangjun Bao*, August 23, 2000, in *FBIS-CHI*, August 23, 2000, p. 2.

59. Matthew J. Von Bencke, *The Politics of Space*, Boulder, CO: Westview Press, 1997, pp. 12, 16, 47, 65.

60. Christoph Bluth, *Soviet Strategic Arms Policy Before SALT*, Cambridge, MA: Cambridge University Press, 1992, pp. 51-58.

61. Qiao Liang and Wang Xiangsui, *Unrestricted Warfare*, Beijing: PLA Literature and Arts Publishing House, February 1999.

62. John Pomfret, "Rewriting the Rules of War: Two Colonels Propose Terrorism, Drugs and Computer Viruses as Strategic Weapons," *Washington Post*, August 16, 1999, p. 15.

63. Kao Chienh-chien, "What Limits has 'Unrestricted Warfare' Exceeded," *Ta Kung Pao*, June 21, 2000, in *FBIS-CHI*, June 21, 2000; and Gao Yan, " Dangerous 'Unrestricted Warfare': And What to Make of the Current International Order and Rules," *Ta Kung Pao*, March 13, 2000, in *FBIS-CHI*, March 13, 2000.

64. Owens, *Lifting the Fog of War*, p. 100.

65. Pillsbury, *China Debates*, pp. 268-275.

66. Dreyer, p. 15.

67. Victor A. DeMarines, "Exploiting the Internet Revolution," in *Keeping the Edge Managing Defense for the Future*, Ashton B. Carter and John P. White, eds., Cambridge, MA: Belfer Center for Science and International Affairs, 2000, pp. 91-92.

68. *Ibid.*, pp. 92-93.

69. Arquilla and Karmel, p. 266.

70. Wang Baocun, "New Military Revolution in the World," *Zhongguo Junshi Kexue*, May 4, 1999, in *FBIS-CHI*, August 23, 1999, p. 6.

71. William C. Triplett II, "Potential Applications of PLA Information Warfare Capabilities to Critical Infrastructures," in *People's Liberation Army After Next*, Susan M. Puska, ed., Carlisle Barracks: U.S. Army War College Strategic Studies Institute, 2000, p. 92.

72. Mulvenon, pp. 183-185.

73. *Ibid.*, p. 185.

74. Rattray, p. 477.

75. John Keegan, *The First World War*, New York: Alfred A. Knopf, 1999, pp. 24-47.

76. Rattray, p. 476.

77. Triplett, p. 80.

78. Ernest R. May, *Strange Victory: Hitler's Conquest of France*, New York: Hill and Wang, 2000, p. 460.

U.S. ARMY WAR COLLEGE

Major General Robert R. Ivany
Commandant

*****

STRATEGIC STUDIES INSTITUTE

Director
Professor Douglas C. Lovelace, Jr.

Director of Research
Dr. Steven Metz

Author
Mr. Toshi Yoshihara

Director of Publications
Ms. Marianne P. Cowling

Publications Assistant
Ms. Rita A. Rummel

*****

Composition
Mrs. Christine A. Williams